Lagrådsremiss

Ny lag om Säkerhetspolisens behandling av personuppgifter

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 29 maj 2019

Mikael Damberg

Peter Lindström
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår att det införs en ny lag om Säkerhetspolisens behandling av personuppgifter som ersätter den tidigare regleringen i polisdatalagen. Den nya lagen föreslås innehålla bestämmelser om bl.a. grundläggande krav på personuppgiftsbehandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, överklagande och överföring av personuppgifter till tredjeland. Dessa överensstämmer i stort sett med brottsdatalagens bestämmelser.

Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. När Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra brott, ska myndigheten tillämpa brottsdatalagen och polisens brottsdatalag. Vidare föreslås följdändringar i ett antal andra lagar.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 januari 2020.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om Säkerhetspolisens behandling av personuppgifter,
2. lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet,
3. lag om ändring i offentlighets- och sekretesslagen (2009:400),
4. lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete,
5. lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning,
6. lag om ändring i säkerhetsskyddslagen (2018:585),
7. lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om Säkerhetspolisens behandling av personuppgifter

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Lagen gäller vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

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

Avvikande bestämmelser i annan författning

4 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Personuppgiftsansvar

5 § Säkerhetspolisen respektive Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Definitioner

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

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.
Dataskyddsombud	Den fysiska person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen.
Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.

Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredjeland	En stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgift som rör hälsa	Personuppgift som rör en per-sons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

Behandling av uppgifter om juridiska personer

7 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 5 § om personuppgiftsansvar,
2. 2 kap. 1 och 2 §§ om rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 och 3 §§ om gemensamt tillgängliga uppgifter,
4. 4 kap. 1–4 och 6–10 §§ om längsta tid som personuppgifter får behandlas, och
5. 5 kap. 5 § om tillgången till personuppgifter.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Rättsliga grunder

1 § Personuppgifter får behandlas om det är nödvändigt för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

a) brott mot Sveriges säkerhet,

b) terrorbrott, eller

c) tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

2. utreda eller lagföra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,

3. fullgöra uppgifter

a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,

b) enligt säkerhetsskyddslagen (2018:585), eller

c) enligt utlännings- och medborgarskapslagstiftningen,

4. fullgöra någon annan uppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen, eller

5. fullgöra förpliktelser som följer av internationella åtaganden.

2 § Utöver vad som sägs i 1 § får personuppgifter behandlas om

1. det är nödvändigt för diarieföring, eller

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

Ändamål

3 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. De får inte behandlas för något ändamål som är oförenligt med det ändamål de ursprungligen behandlades för.

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

1. för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:1177) hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket,

2. i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,

3. i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelseverksamhet, om det finns särskilda skäl att tillhandahålla informationen,

4. i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med en viss uppgift,

5. i brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller

6. i verksamhet hos utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter som behandlas med stöd av 1 § får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra.

I ett enskilt fall får personuppgifter som behandlas med stöd av 1 § även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första och andra styckena, under förutsättning att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

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

Författningsenlig och korrekt behandling

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

Personuppgifternas kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

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

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Känsliga personuppgifter

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

Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket om det är absolut nödvändigt för ändamålet med behandlingen.

10 § Säkerhetspolisen får behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen. Genetiska uppgifter får inte behandlas.

11 § Personuppgifter som avses i 9 och 10 §§ (känsliga personuppgifter) får alltid behandlas med stöd av 2 §.

12 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Första stycket hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Första stycket hindrar inte heller sökningar i syfte att få fram ett urval av personer grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för något av de syften som anges i 1 §.

Rättelse, uppdatering och radering

13 § Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter

lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

14 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–10 § utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

Utlämnande av personuppgifter

15 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

16 § Om det är förenligt med svenska intressen får personuppgifter lämnas ut till

1. Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att mottagaren ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, eller
2. en utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

17 § Polismyndigheten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som behandlas med stöd av 1 § första stycket 1–3 a och c, om myndigheten behöver uppgifterna för ett syfte som anges i 2 kap. 1 § första stycket 1 eller 2 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller för att fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (1991:572) om särskild utlänningskontroll.

18 § Försvarsmakten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som behandlas med stöd av 1 § första stycket 1 eller 2, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst. Detsamma gäller Försvarets radioanstalt, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet.

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

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 5–7 §§.

Personuppgifter från transportföretag

20 § Personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen (1984:387) får behandlas för att utföra en uppgift som anges i 1 §.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål.

21 § Vid terminalåtkomst enligt 26 § polislagen (1984:387) får personuppgifterna inte ändras eller bearbetas på annat sätt.

Rätt att meddela föreskrifter

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

1. att personuppgifter får lämnas ut i andra fall än som anges i 15–18 §§, och
2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 19 § första stycket.

3 kap. Gemensamt tillgängliga uppgifter

Allmän bestämmelse

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga med stöd av 2 §. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 §.

Personuppgifter som får göras gemensamt tillgängliga

2 § Personuppgifter får göras gemensamt tillgängliga om det behövs för att utföra någon av de uppgifter som anges i 2 kap. 1 §.

Särskilda upplysningar

3 § Om det ändamål som de gemensamt tillgängliga personuppgifterna behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

4 § Om uppgifter som har gjorts gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 eller 2, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha direkt samband med sådan brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av omständigheterna är onödigt.

Någon upplysning enligt andra stycket behöver inte heller lämnas om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till, och

2. bearbetningen av uppgifterna inte har genomförts.

Direktåtkomst

5 § Polismyndigheten får för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller för att fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (1991:572) om särskild utlänningskontroll medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1–3 a och c. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

6 § Försvarsmakten får i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 eller 2. Detsamma gäller Försvarets radioanstalt i försvarsunderrättelseverksamheten. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

7 § En underrättelse- eller säkerhetstjänst i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 b om det behövs för samarbetet mot terrorism. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Säkerhetspolisen informera regeringen.

Rätt att meddela föreskrifter

8 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomst enligt 5–7 §§ och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Vid automatiserad behandling gäller också de begränsningar som följer av 2–11 §§.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 § Personuppgifter som inte har gjorts gemensamt tillgängliga får inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller
2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Bestämmelsen i 1 § andra stycket gäller inte vid tillämpningen av denna paragraf.

Första stycket gäller inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifter som finns i anmälan och som har gjorts gemensamt tillgängliga inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifter som har gjorts gemensamt tillgängliga inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

4 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifter som finns i förundersökningen och som har gjorts gemensamt tillgängliga inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts ner eller avslutats på annat sätt än genom åtal, får personuppgifter i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

5 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga gemensamt tillgängliga uppgifter

6 § Andra personuppgifter än de som anges i 3 eller 4 § och som har gjorts gemensamt tillgängliga får som längst behandlas under den tid som anges i 7–10 §§.

Bestämmelsen i 1 § andra stycket gäller inte vid tillämpningen av 7–10 §§.

7 § Personuppgifter får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge, om någon ny registrering inte gjorts efter det att han eller hon fyllt 18 år.

Första och andra styckena gäller inte sådana personuppgifter som avses i 8 och 9 §§.

8 § Personuppgifter som behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket får inte behandlas längre än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

9 § Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt, får inte behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. För personuppgifter som behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket gäller 8 §.

10 § Om det finns särskilda skäl och uppgifterna fortfarande behövs för det ändamål de behandlas för, får Säkerhetspolisen besluta att personuppgifter får behandlas under längre tid än vad som anges i 7–9 §§. Om personuppgifter behandlas med stöd av ett sådant beslut ska frågan om fortsatt behandling prövas på nytt senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i 8 §, senast vid utgången av det tredje kalenderåret efter beslutet. Tiden som personuppgifterna får behandlas får vid varje tillfälle förlängas med längst tio år eller, om det är fråga om uppgifter som avses i 8 §, med längst tre år.

Rätt att meddela föreskrifter

11 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3 och 4 §§.

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

1. att personuppgifter får behandlas för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i 2 § första stycket eller 7–10 §, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Skyldigheter som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

1 § Säkerhetspolisen ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

2 § Säkerhetspolisen ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

3 § Säkerhetspolisen ska se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

4 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

5 § Säkerhetspolisen ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

6 § Om en typ av ny behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Säkerhetsåtgärder

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

Samarbete med tillsynsmyndigheten

8 § Säkerhetspolisen ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Dataskyddsombud

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

10 § Dataskyddsombud ska

1. självständigt kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge Säkerhetspolisen råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

Personuppgiftsbiträden

11 § Säkerhetspolisen får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på myndighetens vägnar. Innan ett personuppgiftsbiträde anlitas ska Säkerhetspolisen försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

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

12 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från Säkerhetspolisen.

13 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen.

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

14 § Det som sägs om Säkerhetspolisens skyldigheter i 4, 5, 7 och 8 §§ gäller även för personuppgiftsbiträden.

6 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Säkerhetspolisen ska göra följande allmänna information tillgänglig för den registrerade:

1. myndighetens identitet och kontaktuppgifter,
2. dataskyddsombudets kontaktuppgifter,
3. kategorier av ändamål för behandlingen,
4. rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av uppgifterna, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 och 7 §§.

Personrelaterad information

2 § Säkerhetspolisen ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden för behandlingen,
4. ändamålen med behandlingen,
5. mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
6. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
7. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 och 7 §§.

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

Begränsning av rätten till information

3 § Informationsskyldigheten i 2 § gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Om förutsättningarna i första stycket är uppfyllda, är Säkerhetspolisen inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 eller 7 §.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,

2. behandlas enbart för vetenskapliga, statistiska eller historiska ändamål, eller

3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

5 § Om en begäran enligt 2 § är orimlig eller uppenbart ogrundad får Säkerhetspolisen avslå den.

Av 9 § andra stycket framgår att Säkerhetspolisen i vissa fall får ta ut avgift i stället för att avslå begäran.

Rätten till rättelse, radering och begränsning av behandlingen

6 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om Säkerhetspolisen inte kan fastställa att personuppgifterna är korrekta, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

7 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne, om de behandlas i strid med 2 kap. 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–10 §. Detsamma gäller om det krävs radering för att Säkerhetspolisen ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska Säkerhetspolisen på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

8 § Säkerhetspolisen avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

9 § Information enligt 1 § ska lämnas utan avgift. Information och uppgifter enligt 2 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 2 § oftare än en gång per år, får Säkerhetspolisen ta ut en rimlig avgift eller avslå begäran enligt 5 § första stycket.

7 kap. Tillsyn

Tillsynsmyndighetens uppgifter

1 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling, och

2. vid förhandssamråd enligt 5 kap. 6 § och när det i övrigt är påkallat ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

2 § Bestämmelser om tillsyn över Säkerhetspolisens behandling av personuppgifter finns även i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

3 § Tillsynsmyndigheten har rätt att av Säkerhetspolisen och personuppgiftsbiträdet på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Förebyggande befogenheter

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

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

Korrigerande befogenheter

5 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att Säkerhetspolisen eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 4 § första stycket försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,
2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller
3. förbjuda fortsatt behandling om bristen är allvarlig.

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

Verkställighet av beslut

6 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

8 kap. Skadestånd och överklagande

Skadestånd

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

Överklagande

Överklagande av den personuppgiftsansvariges beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 6 kap. 6 § första stycket, radering enligt 6 kap. 7 § första stycket, eller begränsning av behandlingen enligt 6 kap. 6 § andra stycket eller 6 kap. 7 § andra stycket, som har meddelats av den personuppgiftsansvarige, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 6 kap. 2 § eller att ta ut avgift enligt 6 kap. 9 § andra stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

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

9 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för överföring

1 § Säkerhetspolisen får överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. riktas till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland eller en internationell organisation med brottsbekämpande uppdrag och
2. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 2 §,

b) tillräckliga skyddsåtgärder enligt 3 §, eller

c) ett undantag för särskilda situationer enligt 4 §.

Beslut om adekvat skyddsnivå

2 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit under de förutsättningar som anges i 1 §. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

3 § Om det inte finns något beslut om adekvat skyddsnivå enligt 2 §, får personuppgifter, under de förutsättningar som anges i 1 §, ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade, eller
2. mottagaren på annat sätt garanterar tillräckligt skydd för personuppgifterna.

Överföring i särskilda situationer

4 § Om det inte finns något beslut om adekvat skyddsnivå enligt 2 § eller tillräckliga skyddsåtgärder enligt 3 §, får en överföring eller en samling av överföringar av personuppgifter, under de förutsättningar som anges i 1 §, göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. värna den registrerades eller någon annan fysisk persons vitala intressen eller andra berättigade intressen som den registrerade har,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Överföring till andra mottagare

5 § Säkerhetspolisen får i ett enskilt fall överföra personuppgifter till en annan mottagare i ett tredjeland än som anges i 1 §. Personuppgifterna får överföras endast om de övriga förutsättningarna i 1 § är uppfyllda och om

1. det är absolut nödvändigt för att Säkerhetspolisen ska kunna utföra en uppgift enligt 2 kap. 1 §, och
2. det skulle vara ineffektivt eller olämpligt att överföra dem till en mottagare som anges i 1 § i det tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs.

---

1. Denna lag träder i kraft den 1 januari 2020.

2. Bestämmelsen i 5 kap. 4 § om loggning tillämpas från och med den 1 oktober 2024 i fråga om automatiserade behandlingssystem som inrättats före ikraftträdandet.

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

2.2 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt prop. 2018/19:96	*Föreslagen lydelse*
1 §	
Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen. *Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 11 § brottsdatalagen.*	Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, *och lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen och 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.*
.	
Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:000) om förbud mot användning av vissa uppgifter för att utreda brott.	
Tillsynen ska särskilt syfta till att säkerställa att verksamheten enligt första, andra och tredje styckena bedrivs i enlighet med lag eller annan författning.	

---

1. Denna lag träder i kraft den 1 januari 2020.
2. Äldre föreskrifter gäller fortfarande för nämndens tillsyn över personuppgiftsbehandling som utförts före ikraftträdandet.

2.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att punkt 2 i ikraftträdande- och övergångsbestämmelserna till lagen (2018:1708) om ändring i den lagen ska upphöra att gälla,

dels att 18 kap. 2 § och 35 kap. 1 och 10 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
2 §[1]	
Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 1 § 1 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.	
Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till sådan verksamhet som avses i	
1. 2 kap. 1 § 1 lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område,	
2. 2 kap. 1 § 1 lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område, *eller*	2. 2 kap. 1 § 1 lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område,
3. 2 kap. 1 § 1 lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdata–lagens område.	3. 2 kap. 1 § 1 lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdata–lagens område, *eller*
	4. 2 kap. 1 § första stycket 1 lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter.
Sekretess enligt första stycket gäller inte för uppgift som hänför sig till verksamhet hos Säkerhetspolisen och som har förts in i en allmän handling före år 1949.	
För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.	

Lydelse enligt prop. 2018/19:65	*Föreslagen lydelse*
35 kap.	
1 §	
Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i	

[1] Senaste lydelse 2018:1708.

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,

3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna,	5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, *eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter,*

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, eller

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Nuvarande lydelse	*Föreslagen lydelse*

10 §[2]

Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut

1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

[2] Senaste lydelse 2018:1716.

2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (2018:585) och i förordning som har meddelats med stöd i den lagen,

3. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken,

4. enligt vad som föreskrivs i

– lagen (1998:621) om misstankeregister,

– lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område

– lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område,

– lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område, *eller*	– lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens *område,*
	– lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter, eller

– förordningar som har stöd i dessa lagar.

Denna lag träder i kraft den 1 januari 2020.

2.4 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

Härigenom föreskrivs att 6 kap. 1 § lagen (2017:496) om internationellt polisiärt samarbete ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
1 §[1]	
Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller brottsdatalagen (2018:1177) och följande författningar för respektive myndighet för behandling av personuppgifter vid internationellt polisiärt samarbete:	Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller brottsdatalagen (2018:1177) och följande författningar för respektive myndighet för behandling av personuppgifter vid internationellt polisiärt samarbete:
– lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,	– lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,
– lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område, *eller*	– lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område,
– lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område.	– lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område, *eller*
	– lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter.

Denna lag träder i kraft den 1 januari 2020.

[1] Senaste lydelse 2018:1714.

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

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

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

Denna lag träder i kraft den 1 januari 2020.

2.6 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs att 3 kap. 13 och 14 §§ säkerhetsskyddslagen (2018:585) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
13 §[1]	
Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister eller lagen (1998:621) om misstankeregister. Med registerkontroll avses också att uppgifter som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens *område* hämtas.	Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister eller lagen (1998:621) om misstankeregister. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av 1. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens *område, eller* 2. *lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter.*
14 §[2]	
Registerkontroll ska göras om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass. Uppgifter ska löpande hämtas under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.	
För säkerhetsklass 1 eller 2 får uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens *område* hämtas. Motsvarande uppgifter får även hämtas om den kontrollerades make eller sambo.	För säkerhetsklass 1 eller 2 får uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område *eller lagen (2019:000) om Säkerhetspolisens behandling av personuppgifter* hämtas. Motsvarande uppgifter får även hämtas om den kontrollerades make eller sambo.
För säkerhetsklass 3 får sådana uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som	För säkerhetsklass 3 får sådana uppgifter om den kontrollerade som finns i belastningsregistret eller misstankeregistret eller som

[1] Senaste lydelse 2018:1715.
[2] Senaste lydelse 2018:1715.

behandlas hos Säkerhetspolisen med stöd av lagen om polisens behandling av personuppgifter inom brottsdatalagens *område* hämtas.	behandlas hos Säkerhetspolisen med stöd av lagen om polisens behandling av personuppgifter inom brottsdatalagens område *eller lagen om Säkerhetspolisens behandling av personuppgifter* hämtas.

Om det finns synnerliga skäl får även andra uppgifter än sådana som anges i andra och tredje styckena hämtas.

Denna lag träder i kraft den 1 januari 2020.

2.7 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs att punkt 4 i ikraftträdande- och övergångsbestämmelserna till lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område ska upphöra att gälla vid utgången av december 2019.

3 Ärendet och dess beredning

Europeiska unionens genomgripande dataskyddsreform omfattar dels 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), i det följande dataskyddsförordningen, dels 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, i det följande dataskyddsdirektivet.

Regeringen beslutade den 17 mars 2016 kommittédirektiv om genomförande av dataskyddsdirektivet (dir. 2016:21). I utredningens uppdrag ingick, förutom att föreslå hur direktivet ska genomföras i svensk rätt, att bedöma om det fanns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat från den lagstiftning som gäller för Polismyndigheten och vid behov lämna författningsförslag. Utredningen om 2016 års dataskyddsdirektiv redovisade den 5 april 2017 delbetänkandet Brottsdatalag (SOU 2017:29), i vilket utredningen föreslog att direktivet i huvudsak skulle genomföras genom en ny ramlag, brottsdatalagen. Regeringen beslutade den 19 april 2018 propositionen Brottsdatalag (prop. 2017/18:232). Lagändringarna trädde i kraft den 1 augusti 2018.

Utredningen redovisade den 4 oktober 2017 slutbetänkandet Brottsdatalag – kompletterande lagstiftning (SOU 2017:74). Den 14 juni 2018 beslutades propositionen Brottsdatalag – kompletterande lagstiftning (prop. 2017/18:269), som behandlar slutbetänkandets förslag till anpassningar och ändringar i de brottsbekämpande myndigheternas registerförfattningar. Lagändringarna trädde i kraft den 1 januari 2019. I denna lagrådsremiss behandlas slutbetänkandets lagförslag om Säkerhetspolisens behandling av personuppgifter.

En sammanfattning av betänkandet i den del som gäller Säkerhetspolisens behandling av personuppgifter finns i *bilaga 1*. Utredningens förslag till en ny lag för Säkerhetspolisens personuppgiftsbehandling finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2017/07698/L4).

4 Säkerhetspolisen

4.1 Säkerhetspolisens uppdrag och verksamhet

Enligt 1 § andra stycket polislagen (1984:387) bedrivs polisverksamhet av Polismyndigheten och Säkerhetspolisen. Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 §. Säkerhetspolisen ska förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott och utreda och beivra sådana brott, fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, fullgöra uppgifter enligt säkerhetsskyddslagen, leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för. I förordningen (2014:1103) med instruktion för Säkerhetspolisen preciseras myndighetens uppdrag.

Säkerhetspolisen är också nationell säkerhetstjänst. En säkerhetstjänst arbetar för att höja säkerhetsnivån i den egna staten. Det görs dels genom att avslöja och reducera säkerhetshot som riktas mot staten, dels genom att reducera sårbarheter. I egenskap av säkerhetstjänst bedriver Säkerhetspolisen underrättelse- och säkerhetsarbete. Myndigheten bedriver omfattande säkerhetsunderrättelseverksamhet för att ta fram hot- och sårbarhetsbedömningar. Verksamheten är inriktad på att avslöja om viss brottslighet kan komma att begås. Bedömningarna tjänar som underlag för beslut om vilka åtgärder Säkerhetspolisen ska vidta i sitt förebyggande arbete. De ligger också till grund för beslut om t.ex. personskydd eller säkerhetsskyddsåtgärder. Ett övergripande mål med säkerhetsunderrättelseverksamheten är att hämta in kunskap som kan omsättas i operativ verksamhet (En tydligare organisation för Säkerhetspolisen, SOU 2012:77, s. 56 f.).

Säkerhetspolisens verksamhet är indelad i fem huvudområden. Kontraspionageverksamheten ska förebygga och avslöja spioneri och annan olovlig underrättelseverksamhet som kan rikta sig mot Sverige och svenska intressen utomlands, mot utländska intressen i Sverige och mot flyktingar. Kontraterrorismverksamheten syftar till att förebygga och avslöja bl.a. terrorism som riktas mot Sverige, svenska intressen utomlands och utländska intressen i Sverige, internationella terroristnätverks förgreningar i Sverige och stöd och finansiering av terroristverksamhet. Den författningsskyddande verksamheten har till uppgift att motverka verksamhet som genom trakasserier, hot, våld, tvång eller korruption syftar till att påverka det demokratiska statsskickets funktioner. Säkerhetspolisen ansvarar även för personskyddet av den centrala statsledningen och främmande statsbeskickningsmedlemmar och vid statsbesök och liknande händelser. Säkerhetspolisen bedriver också säkerhetsskyddsverksamhet, som syftar till att höja säkerhetsnivån i samhället genom analyser,

registerkontroller, tillsyn och rekommendationer till myndigheter vilkas verksamhet har betydelse för Sveriges säkerhet.

Säkerhetspolisen har också vissa uppgifter enligt utlännings- och medborgarskapslagstiftningen. Enligt 1 kap. 7 § utlänningslagen (2005:716) är säkerhetsärenden ärenden där Säkerhetspolisen av skäl som rör rikets säkerhet eller som annars har betydelse för allmän säkerhet förordar att vissa beslut ska meddelas, exempelvis att en utlänning ska avvisas eller utvisas eller att en utlännings ansökan om uppehållstillstånd ska avslås. Säkerhetspolisen har rätt att överklaga Migrationsverkets beslut i sådana ärenden. Säkerhetspolisen är också verkställande myndighet i säkerhetsärenden, vilket ger myndigheten rätt att fatta beslut i frågor om förvar och uppsikt. Säkerhetspolisen har även uppgifter enligt lagen (1991:572) om särskild utlänningskontroll. Med stöd av den lagen kan myndigheten ansöka om att en utlänning ska utvisas ur landet. Säkerhetspolisen ansvarar för att beslut om utvisning enligt lagen verkställs. Enligt lagen (2001:82) om svenskt medborgarskap kan Säkerhetspolisen förorda att en ansökan om svenskt medborgarskap ska avslås av skäl som rör rikets säkerhet eller allmän säkerhet. Myndigheten har även rätt att överklaga sådana beslut.

Säkerhetspolisen arbetar även med frågor som rör ickespridning. Den verksamheten syftar till att förhindra spridning och anskaffning av produkter som kan användas för att producera massförstörelsevapen. Arbetet går främst ut på att förhindra att kunskaper, produkter, ämnen eller mikroorganismer förs från eller via Sverige till aktörer som har ambitioner att anskaffa eller vidareutveckla massförstörelsevapen.

Säkerhetspolisen samverkar med Polismyndigheten inom vissa områden, exempelvis verkställighet av hemlig rumsavlyssning och hemliga tvångsmedel på teleområdet.

4.2 Säkerhetspolisens organisation

Säkerhetspolisen blev den 1 januari 2015 en fristående myndighet. Myndigheten leds av en säkerhetspolischef, som är generaldirektör, och en biträdande säkerhetspolischef. De biträds av generaldirektörens stab.

Sedan den 1 oktober 2016 är Säkerhetspolisens kärnverksamhet uppdelad i två avdelningar; säkerhetsunderrättelseavdelningen och säkerhetsavdelningen. Den förstnämnda ansvarar för myndighetens säkerhetsunderrättelseverksamhet, dvs. arbetet med att bedöma och reducera hotaktörers avsikt och förmåga att bedriva säkerhetshotande verksamhet. Avdelningen ansvarar även för brottsutredningar och ärenden enligt utlännings- och medborgarskapslagstiftningen. Där bedrivs också underrättelsearbete med främsta syfte att förse myndigheten med beslutsunderlag för säkerhetsåtgärder. Säkerhetsavdelningen ansvarar för verksamhet inom områdena säkerhetsskydd och personskydd och för det interna säkerhetsarbetet och den interna riskhanteringen.

Det finns också en inhämtningsavdelning, en informations- och utvecklingsavdelning och en avdelning för verksamhetsstöd. Inhämtningsavdelningen utför på uppdrag av säkerhets- eller säkerhetsunderrättelseavdelningen inhämtnings- eller åtgärdsuppdrag. Avdelningen ansvarar för

operativ stödverksamhet avseende bl.a. hemliga tvångsmedel. Vid avdelningen finns också myndighetens funktion för finansiella underrättelser och Säkerhetspolisens ledningscentral. Informations- och utvecklingsavdelningen ansvarar för myndighetens samlade informationsförsörjning genom att registrera och grundbearbeta den information som kommer in till myndigheten och göra den tillgänglig för övriga delar av myndigheten. Avdelningen samordnar utvecklingsarbetet avseende bl.a. systemförvaltning. Avdelningen för verksamhetsstöd ansvarar för Säkerhetspolisens administrativa verksamhet som rör bl.a. personal och ekonomi.

5 Dagens reglering av behandling av personuppgifter

5.1 Grundläggande reglering om skydd av den personliga integriteten

Regeringsformen och Europakonventionen

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. Inskränkningar i detta skydd får enligt 2 kap. 20 och 21 §§ regeringsformen enbart göras genom lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle.

Grundlagsskyddet omfattar enbart betydande intrång. I förarbetena till ändringen framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses det allmännas hantering av uppgifterna normalt vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget (En reformerad grundlag, prop. 2009/10:80, s. 183). Konstitutionsutskottet har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållit att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll ska regleras särskilt i lag (se bl.a. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 43).

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som svensk lag (SFS 1994:1219). Enligt artikel 8 har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i dessa rättigheter får endast göras med stöd av lag och för vissa i artikeln uppräknade ändamål, bl.a. hänsyn till den allmänna säkerheten och förebyggande av oordning och brott. Artikel 8 skyddar bl.a. mot felaktig behandling av personuppgifter (se Segerstedt-Wiberg m.fl. mot Sverige, Ansökan 62332/00, dom den 6 juni 2006).

Även Europeiska unionens (EU) stadga om de grundläggande rättigheterna (rättighetsstadgan) innehåller bestämmelser om behandling av personuppgifter.

Dataskyddskonventionen

Europarådets ministerkommitté antog 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen (nr 108). Konventionen trädde i kraft den 1 oktober 1985. I syfte att modernisera konventionen har en översyn av den pågått inom Europarådet. Förhandlingarna resulterade i maj 2018 i att ett ändringsprotokoll antogs och Sverige tillhörde de första konventionsstaterna att underteckna protokollet. Processen för att ändringsprotokollet ska träda i kraft har därmed inletts. Konventionens syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter. Utgångspunkten är att vissa av den enskildes rättigheter kan behöva skyddas i förhållande till den princip om fritt flöde av information, oberoende av gränser, som finns inskriven i internationella överenskommelser om mänskliga rättigheter. Konventionens tillämpningsområde är enligt huvudregeln automatiserade personregister och automatisk databehandling av personuppgifter i allmän och enskild verksamhet.

I konventionen anges krav på de personuppgifter som är föremål för automatisk databehandling, bl.a. krav på att uppgifterna ska hämtas in och behandlas på ett korrekt sätt och vara relevanta med hänsyn till ändamålet, att vissa typer av uppgifter inte får behandlas automatiserat om inte nationell lagstiftning ger ett ändamålsenligt skydd och att lämpliga säkerhetsåtgärder ska vidtas för att skydda personuppgifter gentemot oavsiktlig eller otillåten förstörelse.

Konventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. En sådan rekommendation rör polisen.

Sverige har, i likhet med övriga medlemsstater i EU, anslutit sig till konventionen.

5.2 Regleringen av Säkerhetspolisens personuppgiftsbehandling

Polisdatalagen

Säkerhetspolisens personuppgiftsbehandling regleras i 6 kap. polisdatalagen (2010:361). Lagen upphörde att gälla den 1 januari 2019, men gäller för Säkerhetspolisens behandling av personuppgifter i frågor som rör nationell säkerhet genom en övergångsreglering (avsnitt 6.3). I kapitlet anges ändamålen för Säkerhetspolisens personuppgiftsbehandling. Det finns även särskilda bestämmelser om behandling av känsliga personuppgifter och om bevarande och gallring. I 6 kap. 4 § hänvisas till ett flertal bestämmelser i 2 kap. som ska tillämpas av Säkerhetspolisen. Bland dem 2 kap. 2 § som i sin tur hänvisar till ett antal bestämmelser i personuppgiftslagen (1998:204) som gäller vid Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen. Det gäller bl.a. definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd. Även personuppgiftlagen har upphört att gälla, men kan tillämpas av Säkerhetspolisen genom en övergångsreglering (avsnitt 6.3).

I polisdataförordningen (2010:1155), som övergångsvis fortfarande gäller för Säkerhetspolisen, finns ytterligare bestämmelser om bl.a. behörighetstilldelning, ändamål, elektroniskt utlämnande och bevarande och gallring.

Ändamål för behandling

I 6 kap. 1–3 §§ polisdatalagen anges för vilka ändamål Säkerhetspolisen får behandla personuppgifter. Ändamålen delas in i primära och sekundära.

De primära ändamålen, som avser behandling av personuppgifter för behoven i Säkerhetspolisens brottsbekämpande verksamhet, anges uttömmande i 6 kap. 1 § polisdatalagen. Personuppgifter får behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terrorbrott eller tryck- eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv. Personuppgifter får även behandlas för att utreda eller beivra sådana brott eller, efter särskilt beslut, annat brott. Säkerhetspolisen får också behandla personuppgifter om det behövs för att fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, fullgöra uppgifter enligt säkerhetsskyddslagen, fullgöra förpliktelser som följer av internationella åtaganden, lämna tekniskt biträde till Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket eller fullgöra annan verksamhet som anges i lag eller förordning eller särskilt beslut av regeringen.

De sekundära ändamålen aktualiseras när personuppgifter som redan behandlas i Säkerhetspolisens brottsbekämpande verksamhet lämnas ut till andra myndigheter eller organisationer för deras behov. Enligt de sekundära ändamålen, som anges i 6 kap. 2 § polisdatalagen, får personuppgifter behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten,

Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket eller hos en utländsk myndighet eller mellanfolklig organisation. Utlämnande är vidare tillåtet om behandlingen är nödvändig för att tillhandahålla information som behövs i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott eller i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst om det finns särskilda skäl att tillhandahålla informationen. Detsamma gäller om Säkerhetspolisen enligt lag eller förordning ska bistå en myndighet med viss uppgift. Säkerhetspolisen får även behandla personuppgifter om det är nödvändigt för att tillhandahålla information till bl.a. riksdagen och regeringen. Personuppgifter får dessutom behandlas för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen). I 12 § polisdataförordningen finns ytterligare bestämmelser om ändamål för utlämnande av personuppgifter.

Personuppgifter får enligt 6 kap. 3 § polisdatalagen också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Utlämnande av personuppgifter

När det gäller utlämnande av personuppgifter och uppgiftsskyldighet gäller bestämmelserna i 2 kap. 14 och 15 §§ polisdatalagen för Säkerhetspolisen. I 14 § föreskrivs att personuppgifter får lämnas ut för att framställa rättsstatistik. I 15 § finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol, Europol, utländsk underrättelse- eller säkerhetstjänst och annan utländsk myndighet eller mellanfolklig organisation.

Även bestämmelserna om elektroniskt utlämnande i 2 kap. 20 och 21 §§ polisdatalagen gäller för Säkerhetspolisen. Där föreskrivs att enstaka personuppgifter får lämnas ut på medium för automatiserad behandling och att utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av lagen. Säkerhetspolisen har inte getts någon möjlighet att lämna ut personuppgifter genom direktåtkomst. I polisdataförordningen finns kompletterande bestämmelser om elektroniskt utlämnande. Där föreskrivs bl.a. att fler än enstaka personuppgifter under vissa förutsättningar får lämnas ut på medium för automatiserad behandling till ett antal angivna myndigheter.

Behandling av känsliga personuppgifter

Bestämmelserna om behandling av känsliga personuppgifter i 2 kap. 10 § polisdatalagen gäller för Säkerhetspolisen. 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 om det är absolut nödvändigt för syftet med behandlingen.

Behandling av gemensamt tillgängliga uppgifter

I 6 kap. 8 § polisdatalagen föreskrivs att personuppgifter får göras gemensamt tillgängliga i Säkerhetspolisen verksamhet om det behövs för de ändamål för vilka Säkerhetspolisen får behandla personuppgifter.

När personuppgifter görs gemensamt tillgängliga ska det, enligt 6 kap. 9 §, genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Om uppgifterna direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet ska det enligt 6 kap. 10 § framgå att personen inte är misstänkt. Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Sådana upplysningar behöver dock inte lämnas om det på grund av särskilda omständigheter är onödigt eller om uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede.

Vid sökning i gemensamt tillgängliga uppgifter får Säkerhetspolisen enligt 6 kap. 11 § polisdatalagen använda känsliga personuppgifter som sökbegrepp endast om det är absolut nödvändigt.

Bevarande och gallring

I 6 kap. 6 § polisdatalagen föreskrivs att Säkerhetspolisen inte får bevara personuppgifter under längre tid än vad som behövs för något eller några av de ändamål som anges i lagen. I 6 kap. 7 och 12–14 §§ regleras hur länge uppgifter längst får bevaras.

Personuppgifter som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter att ärendet avslutats. Om uppgifterna inte kan hänföras till ett ärende ska de gallras senast ett år efter att de behandlades automatiserat första gången.

Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Särskilda regler gäller för personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har tillgång till. Sådana personuppgifter ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om det finns särskilda skäl får Säkerhetspolisen besluta att personuppgifter får bevaras längre tid om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas.

Annan tillämplig lagstiftning

Säkerhetspolisen tillämpar också lagen (2017:496) om internationellt polisiärt samarbete och föreskrifter som har meddelats i anslutning till den lagen. Lagen tillämpas på polisiärt samarbete mellan Sverige och andra stater i den utsträckning som Sverige i en internationell överenskommelse har gjort sådana åtaganden som avses i lagen. För Säkerhetspolisen behandling av personuppgifter vid internationellt polisiärt samarbete gäller polisdatalagen, om inte annat följer av lagen om internationellt

polisiärt samarbete eller förskrifter som regeringen har meddelat i anslutning till den lagen.

I 7–9 kap. lagen om internationellt polisiärt samarbete regleras informationsutbyte enligt vissa EU-rättsakter; Prümrådsbeslutet, CBE-direktivet och VIS-rådsbeslutet. I 10 kap. regleras uppgiftsutbyte enligt avtalet med USA.

6 Europeiska unionens dataskyddsreform

6.1 Två nya rättsliga instrument

Den allmänna regleringen av behandling av personuppgifter inom EU har sedan länge funnits i 1995 års dataskyddsdirektiv, vilket genomfördes genom personuppgiftslagen (1998:204). Efter flera års förhandlingar enades Europaparlamentet och rådet den 27 april 2016 om en ny reglering av skyddet för enskilda vid behandling av personuppgifter. Den består av två rättsliga instrument. Det ena är dataskyddsförordningen och det andra är dataskyddsdirektivet. Viss behandling av personuppgifter undantas från både dataskyddsförordningens och dataskyddsdirektivets tillämpningsområden. Det gäller personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

6.2 Dataskyddsförordningen och dataskyddslagen

Dataskyddsförordningen utgör sedan den 25 maj 2018 den generella regleringen av personuppgiftsbehandling inom EU. Förordningen ersätter 1995 års dataskyddsdirektiv och baseras till stor del på den struktur och reglering som finns i det direktivet. I förordningen regleras bl.a. grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, tillsyn över personuppgiftsbehandling och rätten för enskilda att få tillgång till rättsmedel. Genom dataskyddsförordningen införs ett nytt system med administrativa sanktionsavgifter som ska tas ut vid överträdelser av förordningen.

Från dataskyddsförordningens tillämpningsområde undantas bl.a. personuppgiftsbehandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Vidare gäller förordningen inte för sådan behandling av personuppgifter som utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff. Sådan personuppgiftsbehandling omfattas i stället av dataskyddsdirektivets tillämpningsområde.

När dataskyddsförordningen började tillämpas upphörde personuppgiftslagen (1998:204) att gälla. Samtidigt trädde lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (i det följande dataskyddslagen) i kraft. Enligt 1 kap. 2 § ska bestämmelserna i dataskyddsförordningen och dataskyddslagen gälla även utanför sitt

egentliga tillämpningsområde, t.ex. i verksamhet som rör nationell säkerhet. Det gäller dock enligt 1 kap. 3 § 3 inte Säkerhetspolisens brottsbekämpande verksamhet. Dataskyddslagen är subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i registerförfattningar. Dataskyddslagen gäller på samma sätt som dataskyddsförordningen inte när dataskyddsdirektivet är tillämpligt.

6.3 Genomförandet av dataskyddsdirektivet

Brottsdatalagen

Dataskyddsdirektivet ska dels skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt. Direktivet ersätter rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Direktivet har i huvudsak genomförts genom en ny ramlag, brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018.

Brottsdatalagen drar upp gränsen mellan å ena sidan den särskilda regleringen av behandling av personuppgifter vid brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet och å andra sidan dataskyddsförordningens tillämpningsområde. Lagen ska tillämpas av dem som är behöriga myndigheter enligt lagen, om syftet med personuppgiftsbehandlingen är att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det är alltså syftet med behandlingen av personuppgifter i det enskilda fallet som blir avgörande för när lagen ska tillämpas, inte i vilken verksamhet behandlingen utförs.

Lagen gäller enbart för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling som ingår i eller är avsedd att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen regleras frågor som är gemensamma för alla behöriga myndigheter. Där finns de grundläggande bestämmelserna om hur personuppgifter får behandlas. Där regleras även personuppgiftsansvarigas skyldigheter, enskildas rättigheter och tillsynen över personuppgiftsbehandling. Brottsdatalagen innehåller vidare bestämmelser om administrativa sanktionsavgifter, skadestånd och rättsmedel. Brottsdatalagen fyller inom sitt tillämpningsområde i stort sett samma funktion som personuppgiftslagen tidigare gjort. Det finns, precis som tidigare, särskilda registerförfattningar för flertalet av de myndigheter som tillämpar brottsdatalagen. Där finns de bestämmelser som är specifika för respektive myndighet.

Ändringar i myndigheternas registerförfattningar

Tillämpningsområdet för registerförfattningarna

Registerförfattningarna för myndigheterna i rättskedjan utgick tidigare från personuppgiftslagen, antingen genom att registerförfattningen gällde i stället för personuppgiftslagen, men hänvisade till bestämmelser i den eller genom att registerförfattningen gällde utöver personuppgiftslagen. Regeringen föreslog i propositionen Brottsdatalag – kompletterande lagstiftning (prop. 2017/18:269) de ändringar i registerförfattningarna som föranleds av införandet av brottsdatalagen. Lagändringarna trädde i kraft den 1 januari 2019. Registerförfattningarna bytte då också namn. Registerförfattningarna gäller utöver brottsdatalagen och innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i den lagen.

Som nyss nämnts är det syftet med personuppgiftsbehandlingen som avgör om brottsdatalagen är tillämplig. Detsamma gäller registerförfattningarnas tillämpningsområde. Tidigare reglerade registerförfattningarna personuppgiftsbehandling såväl i myndigheternas kärnverksamhet som för att lämna uppgifter till andra – oavsett för vilket ändamål det gjordes. I dag reglerar registerförfattningarna enbart den personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde. Det är en direkt effekt av att olika regelverk gäller för personuppgiftsbehandling inom brottsdatalagens respektive dataskyddsförordningens tillämpningsområden.

Övergångsreglering styr Säkerhetspolisens personuppgiftsbehandling

Den 1 januari 2019 upphävdes polisdatalagen samtidigt som lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, hädanefter polisens brottsdatalag, trädde i kraft. I förarbetena till polisens brottsdatalag ansåg regeringen att Säkerhetspolisens behandling av personuppgifter på området för nationell säkerhet inte skulle regleras i den lagen utan regleras på annat sätt (prop. 2017/18:269 s. 285). I avvaktan på ett sådant regelverk, gäller polisdatalagen i dess äldre lydelse för Säkerhetspolisens behandling av personuppgifter i frågor som rör nationell säkerhet. I de delar polisdatalagen hänvisar till personuppgiftslagen fortsätter även den lagen att gälla för Säkerhetspolisen. Även vissa äldre bestämmelser i offentlighets- och sekretesslagen (2009:400), säkerhetsskyddslagen (2018:585) och lagen (2017:496) om internationellt polisiärt samarbete fortsätter övergångsvis att gälla för Säkerhetspolisen (prop. 2017/18:269 s. 285).

7 En ny lag och dess tillämpningsområde

7.1 En särskild lag för Säkerhetspolisens personuppgiftsbehandling

Regeringens förslag: Det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter. När personuppgifter behandlas enligt den nya lagen ska lagen med kompletterande bestämmelser till EU:s dataskyddsförordning inte gälla.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag. Utredningen föreslår att den nya lagen ska benämnas Säkerhetspolisens datalag och att den nya lagen ska innehålla en bestämmelse om förhållandet till dataskyddförordningen och dataskyddslagen.

Remissinstanserna: De flesta remissinstanser tillstyrker förslaget eller har inget att invända mot det.

Skälen för regeringens förslag

Säkerhetspolisen är en fristående myndighet

Vid polisdatalagens tillkomst var Säkerhetspolisen en avdelning vid Rikspolisstyrelsen. Den tidigare gällande polisdatalagen (1998:622) gällde vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Vid den numera upphävda polisdatalagens tillkomst ansåg regeringen att detsamma borde gälla för den lagen (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 71). Regeringen framhöll att Säkerhetspolisens verksamhet i stor utsträckning bedrivs på liknande sätt som annan polisverksamhet och att den reglering som föreslogs för polisen i övrigt därför i många avseenden borde tillämpas även av Säkerhetspolisen. I förarbetena konstaterades dock att särdragen i Säkerhetspolisens verksamhet motiverade att vissa bestämmelser utformades på ett sätt som var mer anpassat till den verksamheten (prop. 2009/10:85 s. 250 f.). Säkerhetspolisens behandling av personuppgifter i den brottsbekämpande verksamheten regleras därför i dag i ett särskilt kapitel i polisdatalagen (avsnitt 5.2).

När Säkerhetspolisen blev en fristående myndighet gjordes det vissa ändringar i polisdatalagen (Den nya polisorganisationen – några frågor om personuppgiftbehandling m.m., prop. 2014/15:94, s. 82 f.). Eftersom Säkerhetspolisens personuppgiftsbehandling var föremål för grundlig översyn när polisdatalagen infördes ansåg regeringen emellertid att det inte fanns något behov av att se över den materiella regleringen (En ny organisation för polisen, prop. 2013/14:110, s. 480 f.). Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten regleras därför även efter omorganisationen i polisdatalagen.

Säkerhetspolisens verksamhet skiljer sig från Polismyndighetens

Även om Säkerhetspolisens och Polismyndighetens verksamhet i stor utsträckning bedrivs på liknande sätt, skiljer sig Säkerhetspolisens uppdrag från Polismyndighetens. Säkerhetspolisen har en betydligt mer begränsad verksamhet, inriktad på några få områden. Tyngdpunkten ligger på att förebygga och förhindra brott. Säkerhetspolisen har i uppdrag att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Säkerhetspolisens verksamhet rör därmed i princip uteslutande nationell säkerhet.

Säkerhetspolisens uppdrag är att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet och terrorbrott och att utreda och beivra sådana brott och vissa andra brott. Arbetet förutsätter att myndigheten har förmåga att identifiera och kartlägga sådan brottslig verksamhet. Säkerhetspolisen behöver kunna behandla personuppgifter på ett tidigt stadium, innan en person eller en gruppering har konkreta brottsplaner eller har vidtagit åtgärder för att begå brott. Säkerhetspolisens arbete är alltså främst inriktat mot att identifiera planer på och förstadier av brottslig verksamhet. När Säkerhetspolisen identifierar brottslig verksamhet i ett så tidigt skede kan brottsligheten normalt förhindras. Då kan konkreta brottsliga gärningar vara svåra att urskilja. Säkerhetspolisens polisiära verksamhet fokuserar alltså på att förebygga och förhindra brott. Det innebär att det finns avgörande skillnader i Säkerhetspolisens verksamhet och arbetsmetoder jämfört med Polismyndighetens.

I motsats till vad som gäller för Polismyndigheten är Säkerhetspolisens brottsutredande verksamhet mycket liten och initieras endast undantagsvis genom anmälningar om brott. Vid misstanke om brott inleds förundersökning, som bedrivs enligt samma regler som gäller för Polismyndigheten. Vid misstanke om vissa brott ska utredningen alltid skötas av Säkerhetspolisen. Det gäller bl.a. spionerі, grovt spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet och vissa tryckfrihets- och yttrandefrihetsbrott. Förundersökningen leds alltid av åklagare. Säkerhetspolisen får även utreda vissa andra brott, men kan avstå från det och överlämna frågan till Polismyndigheten. Under en förundersökning har Säkerhetspolisen samma befogenheter som Polismyndigheten och kan genomföra exempelvis husrannsakan och förhör i syfte att få fram ett tillräckligt beslutsunderlag för åklagaren.

Brottsdatalagen gäller inte Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet

Brottsdatalagen ska enligt 1 kap. 2 § gälla vid behandling av personuppgifter som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Enligt 1 kap. 4 § gäller lagen dock inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Till Säkerhetspolisens huvuduppgifter hör som nyss nämnts att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott

mot Sveriges säkerhet och terrorbrott och att utreda och beivra sådana brott. Säkerhetspolisen ansvarar vidare för personskyddet av den centrala statsledningen. De uppgifterna avser nationell säkerhet. Säkerhetspolisen har även andra uppgifter som avser nationell säkerhet eller som har mycket nära samband med sådan verksamhet. Den absoluta merparten av Säkerhetspolisens behandling av personuppgifter ligger härigenom utanför brottsdatalagens tillämpningsområde (jfr Brottsdatalag, prop. 2017/18:232, s. 103).

En ny lag bör införas

Det nationella regelverket för personuppgiftsbehandling har förändrats. Brottsdatalagen har införts och myndigheternas registerförfattningar har anpassats till denna. Vidare har polisdatalagen upphävts. Säkerhetspolisen tillämpar därför i dag en övergångsreglering för behandling av personuppgifter som rör nationell säkerhet (avsnitt 6.3). Varken brottsdatalagen eller polisens brottsdatalag gäller för Säkerhetspolisen behandling av personuppgifter som rör nationell säkerhet. Säkerhetspolisen har enligt regeringens bedömning ett lika stort behov av särregler för sin personuppgiftsbehandling i dag som tidigare. Med hänsyn till detta och till att Säkerhetspolisen numera är en fristående myndighet, anser regeringen att det bör införas en ny lag som reglerar Säkerhetspolisens personuppgiftsbehandling.

Lagens benämning

Utredningen föreslår att den nya lagen ska benämnas Säkerhetspolisens datalag. När det gäller de registerförfattningar som ska gälla utöver brottsdatalagen föreslog utredningen att de skulle ges enhetliga benämningar som knöt an till brottsdatalagen, exempelvis polisens brottsdatalag och Tullverkets brottsdatalag. Lagrådet anslöt sig till utredningens förslag. Regeringen konstaterade dock att de föreslagna namnen avvek från hur svenska författningar normalt benämns och följaktligen skulle bryta mot den systematik som gäller för författningars rubriker (Ds 2014:1 s. 17 f.). Regeringen ansåg därför att lagarna skulle ges namn som anger för vem författningen gäller och vad den handlar om, exempelvis lagen om polisens behandling av personuppgifter inom brottsdatalagens område och lagen om Tullverkets behandling av personuppgifter inom brottsdatalagens område (prop. 2017/18:269 s. 143 f. och 173 f.). På samma sätt som i förarbetena till de lagarna används här namnet polisens brottsdatalag i löptexten.

Mot den bakgrunden bör den nya lagen inte ges det namn som utredningen föreslår. Eftersom Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet undantas från brottsdatalagens tillämpningsområde kan namnet inte på samma sätt som övriga brottsbekämpande myndigheters registerförfattningar kopplas till brottsdatalagen. Namnet bör vara så enkelt och tydligt som möjligt. Samtidigt bör det återspegla lagens innehåll. Den bör därför benämnas lagen om Säkerhetspolisens behandling av personuppgifter, i det följande Säkerhetspolisens datalag.

Regleringen ska utgå från regleringen i polisdatalagen och brottsdatalagen

Regleringen i polisdatalagen av Säkerhetspolisens personuppgiftsbehandling är relativt ny och har i allt väsentligt fungerat som avsetts. Bestämmelserna i polisdatalagen bör därför till stor del kunna bilda mönster för bestämmelserna i den nya lagen. Då den nya lagen ska vara heltäckande kommer den dock att bli betydligt mer omfattande än den nuvarande regleringen för Säkerhetspolisen. Lagen bör därför indelas i kapitel. Det kan också finnas skäl att överväga om några av de nya bestämmelserna i polisens brottsdatalag även bör tas in i den nya lagen.

Eftersom varken dataskyddsdirektivet eller dataskyddsförordningen omfattar behandling av personuppgifter som utförs i verksamhet som rör nationell säkerhet finns det ur EU-rättslig synvinkel inte något som hindrar att den nya lagen utformas på annat sätt än brottsdatalagen. Enligt regeringens mening bör ändå särregleringen för Säkerhetspolisen följa brottsdatalagens systematik och innehåll om det inte finns skäl att välja en annan lösning med hänsyn till särdragen i Säkerhetspolisens verksamhet. Att reglerna så långt möjligt stämmer överens underlättar tillämpningen både för Säkerhetspolisen och för tillsynsmyndigheten.

Den EU-rättsliga regleringen, som brottsdatalagen och polisdatalagen härrör från, bygger också på och vidareutvecklar dataskyddskonventionen. Konventionen gäller även i verksamhet som rör nationell säkerhet och Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. En särreglering av Säkerhetspolisens personuppgiftsbehandling får således inte strida mot bestämmelserna i dataskyddskonventionen. Genom att den nya lagen utgår från polisdatalagen och brottsdatalagen bedöms regleringen vara förenlig med dataskyddskonventionen och dess tilläggsprotokoll.

Förhållandet till dataskyddsförordningen

Dataskyddsförordningen ska enligt artikel 2.2 a inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. I skäl 16 anges verksamhet rörande nationell säkerhet som exempel på sådan verksamhet. Enligt 1 kap. 2 § dataskyddslagen utsträcks emellertid tillämpningen av dataskyddsförordningen och dataskyddslagen till att gälla även i verksamhet som inte omfattas av unionsrätten. I förarbetena till bestämmelsen anges det dock att det med hänsyn till rikets säkerhet inte är lämpligt att låta dataskyddsförordningen bli tillämplig även inom de mest känsliga verksamhetsområdena innan den pågående översynen av författningarna på försvarsområdet och beredningen av förslagen rörande Säkerhetspolisens personuppgiftsbehandling har avslutats (Ny dataskyddslag, prop. 2017/18:105, s. 31 f.). Mot den bakgrunden undantas enligt 1 kap. 3 § dataskyddslagen bl.a. verksamhet som omfattas av 6 kap. polisdatalagen från det utsträckta tillämpningsområdet.

Säkerhetspolisens verksamhet är sådan att myndighetens personuppgiftsbehandling bör regleras särskilt i en ny lag. Undantaget i dataskyddslagen bör därför hänvisa till verksamhet som omfattas av den nya lagen. Med hänsyn till att förhållandet mellan den nya lagen och dataskyddsförordningen och dataskyddslagen tydliggörs i dataskyddslagen finns det inte

behov av att, som utredningen föreslår, i den nya lagen ange hur den förhåller sig till dataskyddsförordningen och dataskyddslagen.

7.2 Lagens syfte

Regeringens förslag: Syftet med lagen ska vara att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att ett syfte med lagen ska vara ”att skydda fysiska personer grundläggande fri- och rättigheter i samband med behandling av personuppgifter”.

Remissinstanserna: Endast *Datainspektionen* yttrar sig i denna del och anser att det bör tydliggöras att ett syfte särskilt ska vara att skydda fysiska personers personliga integritet vid behandling av personuppgifter.

Skälen för regeringens förslag: I registerförfattningar förekommer ibland bestämmelser som anger lagens övergripande syfte. Enligt 1 kap. 1 § brottsdatalagen är syftet med lagen att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Bestämmelser om syftet med en reglering saknar normalt egentligt materiellt innehåll. Det har dock inte enbart en symbolisk eller informativ betydelse att uttryckligen slå fast en lags syfte. Att en lags syfte uttryckligen anges kan få relevans i rättstillämpningen genom att det ger vägledning för tolkningen av de materiella bestämmelserna i lagen (prop. 2017/18:232 s. 73 f.). Regeringen delar därför utredningens bedömning att det finns skäl att i den nya lagen ta in en bestämmelse om lagens syfte så att det tydligt framgår att regleringen har dubbla syften.

Att fysiska personers grundläggande rättigheter och friheter ska skyddas vid behandling av personuppgifter är en central målsättning för regleringen. Samtidigt är vissa intrång i den personliga integriteten nödvändiga för att Säkerhetspolisen ska kunna utföra sitt uppdrag och sina uppgifter. Regleringen bör därför ge uttryck för en väl avvägd balans mellan, å ena sidan, skyddet för den personliga integriteten, och, å andra sidan, samhällets behov av att Säkerhetspolisen kan behandla personuppgifter i den verksamhet som omfattas av lagens tillämpningsområde. Regeringen anser därför, till skillnad från *Datainspektionen*, att den dubbla målsättningen och balansen mellan de olika intressena bäst tillgodoses och uttrycks genom en bestämmelse som föreskriver att lagens syfte är att skydda fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att samtidigt säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter.

7.3 Avgränsning av tillämpningsområdet

Regeringens förslag: Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

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

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* efterfrågar en definition av uttrycket nationell säkerhet. *Datainspektionen* anser att begreppet nationell säkerhet bör ersättas med ett tydligare begrepp av vilket framgår att det rör Sveriges säkerhet såväl direkt som indirekt. *Dataskydd.net* anser att begreppet nationell säkerhet bör snävas in.

Skälen för regeringens förslag

Lagen ska gälla för behandling av personuppgifter som rör nationell säkerhet

I 1 kap. 4 § brottsdatalagen undantas Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet från brottsdatalagens tillämpningsområde. Frågan är om begreppet nationell säkerhet bör användas för att avgränsa tillämpningsområdet för den nya lagen eller om det finns skäl att, som *Datainspektionen* anser, välja ett annat begrepp.

I 19 kap. brottsbalken används numera begreppet Sveriges säkerhet, vilket ersatte det äldre begreppet rikets säkerhet. När begreppet byttes ut konstaterade regeringen att innebörden av vad som betraktas som rikets säkerhet hade förändrats och fått ett vidare tillämpningsområde (Förstärkt skydd mot främmande makts underrättelseverksamhet, prop. 2013/14:51, s. 20 och 36). I den nya säkerhetsskyddslagen används också begreppet Sveriges säkerhet (En ny säkerhetsskyddslag, prop. 2017/18:89, s. 41 f.). Ett alternativ skulle därför vara att använda det begreppet även i den nya lagen.

Uttrycket Sveriges säkerhet kan dock vara snävare än nationell säkerhet. En fråga som rör nationell säkerhet i något av våra grannländer kan t.ex. vara av den karaktären att den även indirekt kan komma att påverka Sveriges säkerhet. När det gäller gränsöverskridande terrorism är det av stor betydelse att Säkerhetspolisen både kan ta emot och lämna information som kan bidra till att förhindra terrorbrott oavsett vilken stats nationella säkerhet som hotas. Om uttrycket Sveriges säkerhet skulle användas i den nya lagen medan nationell säkerhet används i brottsdatalagen finns det därför risk för att viss personuppgiftsbehandling i Säkerhetspolisens brottsbekämpande verksamhet skulle falla utanför båda regelverken och i stället omfattas av dataskyddsförordningens tillämpningsområde. För att undvika det bör därför samma uttryck som i brottsdatalagen användas för att avgränsa tillämpningsområdet i den nya lagen.

Polismyndigheten efterfrågar en definition av vad som avses med uttrycket nationell säkerhet. En definition skulle kunna underlätta bedömningen av när lagen är tillämplig. I förarbetena till brottsdatalagen framgår att det rör sig om ett EU-rättsligt begrepp som avgränsar EU:s kompetens gentemot medlemsstaterna och att det i förlängningen är upp till EU-domstolen att avgöra begreppets närmare innebörd (prop. 2017/18:232 s. 104). Mot den bakgrunden ansågs det inte lämpligt att definiera uttrycket nationell säkerhet inom ramen för det lagstiftningsärendet. Det finns inte skäl att nu göra någon annan bedömning.

Lagen ska gälla vid behandling av personuppgifter i den brottsbekämpande och lagförande verksamheten

Brottsdatalagens tillämpningsområde avgränsas framför allt genom syftet med behandlingen. Det beror på att dataskyddsdirektivets tillämpningsområde är avgränsat på det sättet (prop. 2017/18:232 s. 82.). I direktivet och dataskyddsförordningen anges att de inte ska tillämpas på behandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten, vilket bl.a. syftar på nationell säkerhet (avsnitt 6.2). Säkerhetspolisens verksamhet ligger därmed som nämnts till allra största delen utanför både direktivets och förordningens tillämpningsområde. Syftet med behandlingen behöver därför inte användas för att avgränsa tillämpningsområdet för den nya lagen. Tillämpningsområdet bör i stället, på samma sätt som i dag, kopplas till Säkerhetspolisens verksamhet.

Frågan är om tillämpningsområdet i den nya lagen bör avgränsas på samma sätt som i polisdatalagen, dvs. genom en hänvisning till brottsbekämpande verksamhet, eller genom någon annan formulering, t.ex. operativ verksamhet.

I förarbetena till polisdatalagen konstaterar regeringen att arbetet inom Säkerhetspolisens olika verksamhetsområden är förebyggande och ytterst syftar till att förhindra att brott begås och att det därför får anses utgöra en del av Säkerhetspolisens brottsbekämpande verksamhet (prop. 2009/10:85 s. 255 f.). Därför räknas samtliga områden där myndigheten bedriver verksamhet upp i 6 kap. 1 § polisdatalagen. Även i senare förarbeten har det uttalats att all verksamhet vid Säkerhetspolisen i någon mån är brottsbekämpande (En ny organisation för polisen, prop. 2013/14:110, s. 480 f.). Det talar för att uttrycket brottsbekämpande verksamhet bör användas även i den nya lagen.

Även om all Säkerhetspolisens verksamhet har ansetts vara i viss utsträckning brottsbekämpande finns det delar av verksamheten som inte har ett lika tydligt brottsbekämpande syfte som övrig verksamhet. Det beror på att Säkerhetspolisen också är en säkerhetstjänst. I den rollen arbetar Säkerhetspolisen för att höja nivån på säkerheten i Sverige. Verksamheten är främst inriktad på att bedöma om viss säkerhetshotande brottslighet kan antas komma att begås. Bedömningarna tjänar som underlag för beslut om vilka åtgärder Säkerhetspolisen vidtar i sitt förebyggande arbete. De ligger också till grund för beslut om t.ex. personskydd för den centrala statsledningen eller säkerhetsskyddsåtgärder. Eftersom verksamheten och åtgärderna är inriktade på att förebygga att säkerhetshot skapas och kan förverkligas kan de indirekt sägas ha brottsbekämpande syfte.

Det kan diskuteras om Säkerhetspolisens roll som säkerhetstjänst gör det lämpligare att använda ett annat uttryck än brottsbekämpning för att avgränsa tillämpningsområdet, t.ex. operativ verksamhet. Ett alternativ skulle kunna vara att låta lagen omfatta brottsbekämpande och annan operativ verksamhet. Inarbetade begrepp bör dock inte ändras om inte starka skäl talar för det. Det har inte framförts några skäl mot att använda uttrycket brottsbekämpande verksamhet. Även om det skulle finnas fördelar med ett annat uttryck anser regeringen, i likhet med utredningen, att övervägande skäl talar för att behålla samma formulering som i dag.

Med brottsbekämpning avses i dag såväl arbetsuppgifterna att förebygga, förhindra och upptäcka brottslig verksamhet som att utreda och beivra brott. I brottsdatalagen görs det emellertid skillnad mellan brottsbekämpning och lagföring. Det beror på att dataskyddsdirektivet är utformat på det sättet. Uppgiften att beivra brott hänförs till lagföring. Brottsbekämpning har därmed i brottsdatalagen fått en snävare innebörd än i dag (prop. 2017/18:232 s. 93 f.). Brottsbekämpning bör ha samma innebörd i den nya lagen. Säkerhetspolisen har enligt sin instruktion i uppgift att även utreda och beivra, dvs. lagföra, vissa typer av brott. Den nuvarande regleringen omfattar således även lagföring. Den nya lagen bör därför gälla personuppgiftsbehandling som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Intern och administrativ verksamhet bör inte omfattas

Säkerhetspolisen har tidigare tillämpat personuppgiftslagen i sin interna och administrativa verksamhet. Som exempel på interna åtgärder är framtagande av interna föreskrifter, handböcker och policydokument Exempel på administrativ verksamhet kan nämnas personalfrågor och ekonomihantering. I dag ska Säkerhetspolisen tillämpa dataskyddsförordningen och dataskyddslagen vid personuppgiftsbehandling i den interna och administrativa verksamheten. Detta eftersom endast personuppgiftsbehandling i verksamhet som omfattas av 6 kap. polisdatalagen undantas från dataskyddsförordningen och dataskyddslagen utvidgade tillämpningsområde (1 kap. 3 § dataskyddslagen). Frågan är om det finns skäl att låta den nya lagen omfatta personuppgiftsbehandling i intern och administrativ verksamhet om behandlingen rör nationell säkerhet? Viss behandling av personuppgifter som utförs i Säkerhetspolisens interna eller administrativa verksamhet kan nämligen vara av sådan karaktär att den gäller nationell säkerhet. Eftersom det inte ska vara möjligt för en annan stat att med hjälp av offentliga uppgifter kunna kartlägga Säkerhetspolisens organisation gäller dock sekretess i större utsträckning än normalt för uppgifter som rör Säkerhetspolisens personal (se t.ex. 15 kap. 2 § och 18 kap. 2 och 5 §§ offentlighets- och sekretesslagen).

Merparten av den personuppgiftsbehandling som sker i intern och administrativ verksamhet hos Säkerhetspolisens får dock antas inte vara av sådan karaktär att den rör nationell säkerhet. Med beaktande av detta och med hänsyn till den sekretessreglering som finns, föreligger inte skäl att låta den nya lagen omfatta personuppgiftsbehandling i intern och administrativ verksamhet ens om behandlingen rör nationell säkerhet.

Helt eller delvis automatiserad behandling

Den nya lagen bör på samma sätt som i dag gälla för behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

7.4 Polismyndigheten ska tillämpa lagen i vissa fall

Regeringens förslag: Polismyndigheten ska tillämpa den nya lagen när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast *Polismyndigheten* yttrar sig i denna del och ser behov av att tydliggöra när myndigheten ska tillämpa den nya lagen.

Skälen för regeringens förslag: Enligt 28 § förordningen (2014:1102) med instruktion för Polismyndigheten ska myndigheten bistå vid polisverksamhet som leds av Säkerhetspolisen om Säkerhetspolisen i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Polismyndigheten ska vidare, i den utsträckning som myndigheterna kommer överens om, lämna tekniskt biträde och annan hjälp till Säkerhetspolisen. Enligt 15 § instruktionen (2014:1103) för Säkerhetspolisen får biträdande säkerhetspolischefen i samråd med chefen för Nationella operativa avdelningen, trots den ansvarsfördelning som annars gäller mellan myndigheterna, i ett enskilt fall bestämma att en förundersökning eller annan uppgift i den brottsbekämpande verksamheten ska lämnas över till Polismyndigheten för fortsatt handläggning.

Eftersom det är fråga om en arbetsuppgift som rör nationell säkerhet när Säkerhetspolisen begär biträde av Polismyndigheten eller överlämnar en arbetsuppgift till myndigheten med stöd av 15 § instruktionen för Säkerhetspolisen, har regeringen ansett att Polismyndigheten inte ska tillämpa brottsdatalagen i vidare utsträckning än vad Säkerhetspolisen skulle ha gjort om uppgiften legat kvar där (prop. 2017/18:232 s. 105 f.). I dessa fall bör Polismyndigheten i stället tillämpa den särreglering som gäller för Säkerhetspolisen. Det bör därför framgå av den nya lagen att den gäller för Polismyndigheten när myndigheten har övertagit en uppgift som rör nationell säkerhet från Säkerhetspolisen. *Polismyndigheten* har efterfrågat ett klargörande av när myndigheten ska tillämpa lagen. Med hänsyn till att det enbart kan bli fråga om att tillämpa lagen i situationer där Säkerhetspolisen begär bistånd av Polismyndigheten eller annars kommer överens med Polismyndigheten om att den myndigheten ska överta en uppgift från Säkerhetspolisen bör det inte råda någon tvekan om när Polismyndigheten ska tillämpa lagen. Något tydliggörande behöver därför inte göras.

7.5 Säkerhetspolisen ska även tillämpa brottsdatalagen

Regeringens bedömning: Det behöver inte framgå av den nya lagen att Säkerhetspolisen i vissa fall ska tillämpa brottsdatalagen med kompletterande lagstiftning.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att den nya lagen ska innehålla en upplysning om att det i brottsdatalagen och polisens brottsdatalag finns bestämmelser om Säkerhetspolisens personuppgiftsbehandling i frågor som inte rör nationell säkerhet.

Remissinstanserna: Endast *Säkerhetspolisen* yttrar sig i denna del och anser att det finns skäl att överväga om inte hela deras brottsbekämpande verksamhet borde undantas från brottsdatalagen.

Skälen för regeringens bedömning

Även om merparten av Säkerhetspolisens personuppgiftsbehandling undantas från brottsdatalagens tillämpningsområde, finns det viss behandling i myndighetens operativa verksamhet som inte rör nationell säkerhet och därför omfattas av den lagen. Som regeringen konstaterar i förarbetena till brottsdatalagen kan därför inte, som *Säkerhetspolisen* vill, myndighetens personuppgiftsbehandling generellt undantas från brottsdatalagens tillämpningsområde (prop. 2017/18:232 s. 105).

Säkerhetspolisen ska enligt 13 § förordningen med instruktion för Säkerhetspolisen bistå vid polisverksamhet som leds av Polismyndigheten om myndigheten i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Säkerhetspolisen ska också lämna tekniskt biträde och annan hjälp till Polismyndigheten i den utsträckning som myndigheterna kommer överens om. När Säkerhetspolisen lämnar sådan hjälp omfattas personuppgiftsbehandlingen av brottsdatalagens tillämpningsområde om den avser brottsbekämpning, lagföring eller verksamhet för att upprätthålla allmän ordning och säkerhet. Säkerhetspolisen bör följaktligen tillämpa brottsdatalagen när den bistår Polismyndigheten i sådan verksamhet. Detsamma gäller om Säkerhetspolisen bistår andra myndigheter i deras brottsbekämpning, t.ex. vid verkställighet av hemliga tvångsmedel. Som exempel kan nämnas att Säkerhetspolisen bistår Polismyndigheten vid verkställighet av hemlig rumsavlyssning.

Enligt 30 § förordningen med instruktion för Polismyndigheten får chefen för Nationella operativa avdelningen i samråd med biträdande säkerhetspolischefen i ett enskilt fall bestämma att en förundersökning eller annan liknande uppgift i den brottsbekämpande verksamheten ska lämnas över till Säkerhetspolisen för fortsatt handläggning. Syftet med bestämmelsen är bl.a. att jävssituationer ska kunna undvikas (prop. 2013/14:110 s. 400). När Säkerhetspolisen med stöd av ett beslut enligt den paragrafen genomför en förundersökning eller utför någon annan uppgift som normalt skulle utföras av Polismyndigheten och som omfattas av brottsdatalagens tillämpningsområde, bör Säkerhetspolisen tillämpa den lagen.

Brottsdatalagen kompletteras för Polismyndighetens del av polisens brottsdatalag. När Säkerhetspolisen biträder eller övertar en arbetsuppgift från Polismyndigheten ska Säkerhetspolisen tillämpa samma reglering. Säkerhetspolisen ska således enligt 1 kap 1 § 3 polisens brottsdatalag tillämpa den lagen i frågor som inte rör nationell säkerhet, om personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller lagföra brott.

Utredningen föreslår att det i den nya lagen ska tas in en bestämmelse som upplyser om att brottsdatalagen och polisens brottsdatalag i vissa fall är tillämpliga för Säkerhetspolisen. Med hänsyn till att det inte bara är dessa författningar som kan vara tillämpliga när personuppgiftsbehandlingen inte rör nationell säkerhet anser regeringen att en sådan bestämmelse inte bidrar till ökad tydlighet. Någon sådan upplysningsbestämmelse bör därför inte tas in i den nya lagen.

7.6 Förhållandet till annan lagstiftning

Regeringens förslag: Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från den nya lagen, ska den bestämmelsen tillämpas.

Utredningens förslag överensstämmer inte med regeringens. Utredningen lämnar inget förslag till generell subsidiaritetsbestämmelse men föreslår en bestämmelse om att den nya lagen inte ska tillämpas om det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen och en bestämmelse om hur lagen förhåller sig till lagen om internationellt polisiärt samarbete.

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt i denna del.

Skälen för regeringens förslag: I det straffprocessuella regelverket finns det åtskilliga bestämmelser om enskildas rätt till insyn i brottsutredningar och straffrättsliga förfaranden. Av särskild betydelse är 23 kap. rättegångsbalken som reglerar den misstänktes insyn under en förundersökning, 20 kap. rättegångsbalken som rör målsäganden och förundersökningskungörelsen (1947:948) som framför allt reglerar underrättelseskyldigheter till misstänkt, målsägande och andra som berörs av en förundersökning. Brottsförebyggande arbete, underrättelseverksamhet, förundersökningar och brottmålsprocesser kan i dag genomföras på ett ändamålsenligt sätt, eftersom dessa regler tillsammans med bestämmelser om sekretess och tystnadsplikt – när det finns skäl för det – begränsar enskildas rätt till information. Dessa regler kan dock komma i konflikt med reglerna om enskildas rätt till information (avsnitt 14.2). För att det ska vara tydligt att de straffprocessuella reglerna har företräde i en sådan situation bör det tas in en bestämmelse i den nya lagen om att den är subsidiär i förhållande till bestämmelser i en annan lag eller en förordning (jfr prop. 2017/18:232 s. 220). Bestämmelsen bör vara generell och inte begränsad enbart till förhållandet till straffprocessuella regler. Mot den bakgrunden saknas det behov av en särskild bestämmelse om hur den nya lagen förhåller sig till lagen och förordningen om internationellt polisiärt samarbete. Eftersom bestämmelser i grundlag

alltid har företräde framför bestämmelser på lägre normgivningsnivå behövs det inte heller någon bestämmelse om förhållandet till 2 kap. tryckfrihetsförordningen. Hur lagen förhåller sig till annan dataskyddsreglering utvecklas i avsnitt 7.1.

7.7 Uttryck i lagen

Regeringens förslag: Vissa av de uttryck som används i den nya lagen ska definieras.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt i denna del.

Skälen för regeringens förslag

Definitionerna i den nya lagen bör så långt möjligt överensstämma med brottsdatalagens definitioner

Genom hänvisningar i 2 kap. 2 § 1 och 6 kap. 4 § 1 polisdatalagen gäller definitionerna i 3 § personuppgiftslagen av vissa uttryck som är centrala vid behandling av personuppgifter för Säkerhetspolisen. Även i den nya lagen bör vissa centrala uttryck definieras.

I 1 kap. 6 § brottsdatalagen definieras vissa uttryck som används i den lagen. Definitionerna överensstämmer i allt väsentligt med definitionerna i dataskyddsförordningen. Säkerhetspolisen kommer att tillämpa både dataskyddsförordningen och brottsdatalagen i delar av sin verksamhet. För att underlätta tillämpningen bör definitionerna i den nya lagen därför så långt möjligt överensstämma med de definitioner som används i brottsdatalagen. Det innebär att motsvarande definitioner som tidigare använts i personuppgiftslagen inte bör användas i den mån de avviker från brottsdatalagens terminologi, trots att de har tillämpats under lång tid och stämmer bättre överens med terminologin i svensk lagstiftning (prop. 2017/18:232 s. 84).

Nedan följer en redogörelse för ett antal centrala definitioner som bör finnas i den nya lagen. Regeringen återkommer till definitionerna av dataskyddsombud (avsnitt 13.3.1), internationell organisation (avsnitt 17.2), personuppgiftsansvarig (avsnitt 13.1.1), personuppgiftsbiträde (avsnitt 13.4.1), tredjeland (avsnitt 17.2) och tredje man (avsnitt 14.3.2).

Behandling av personuppgifter

I brottsdatalagen avses med behandling av personuppgifter en åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring. Uttrycket omfattar alla åtgärder som vidtas med personuppgifter. Uttrycket är centralt och definitionen bör var densamma som i brottsdatalagen.

Biometriska uppgifter

Varken 1995 års dataskyddsdirektiv eller personuppgiftslagen innehåller någon definition av biometriska uppgifter. Inte heller i andra författningar finns det någon sådan definition, men uttrycket biometriska data används i bl.a. passlagen (1978:302).

Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras (jfr propositionen Fingeravtryck i pass, prop. 2008/09:132, s. 6 f.). När det gäller pass är det framför allt mönster av fingeravtryck, ansiktsgeometri och ögats iris som används, men även regnbågshinna, näthinna, röst, hand, blodkärl, dna eller gång går att använda. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Dessa uppgifter kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet.

Biometriska uppgifter definieras i brottsdatalagen som personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga. Definitionen bör användas även i den nya lagen.

Fotografier och filmer som inte bearbetas tekniskt i syfte att åstadkomma unik identifiering faller utanför definitionen. Bearbetning av bilder av personer för att förbättra bildkvaliteten, förstärka detaljer och liknande omfattas alltså inte. Om bilder däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram i syfte att identifiera personer omfattas de av definitionen. Det kan även anmärkas att sådana personuppgifter, t.ex. fingeravtryck, som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska uppgifter däremot inte i sig utgör biometriska uppgifter.

Definitionen omfattar Säkerhetspolisens hantering av fingeravtryck. Fingeravtryck som har tagits med stöd av rättegångsbalken eller lagen (1991:572) om särskild utlänningskontroll får behandlas i de fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 5 kap. 11 § polisens brottsdatalag. Uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person får också behandlas om uppgiften kommit fram vid utredning om brott. Även oidentifierade fingeravtryck omfattas således av definitionen av biometriska uppgifter, eftersom det är möjligt att med hjälp av dem identifiera personen som har avsatt dem.

Genetiska uppgifter

Genetiska uppgifter definieras inte i 1995 års dataskyddsdirektiv eller i personuppgiftslagen. Med genetiska uppgifter avses i brottsdatalagen personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga. All information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från t.ex. en brottsplats eller ett prov från människokroppen omfattas av definitionen. En motsvarande definition bör tas in i den nya lagen.

Genetiska uppgifter behandlas vid dna-analyser i forensisk verksamhet för att ta fram dna-profiler eller forensiska uppslag. Behandlingen kan avse genetiska uppgifter från såväl identifierade som oidentifierade personer. Eftersom nedärvda eller förvärvade genetiska kännetecken för en person kan framgå av ett spår som påträffas vid utredning av ett brott, omfattas även analys av spåren av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Själva dna-profilen, som behandlas i framför allt Polismyndighetens dna-register, är endast en sifferkombination och därmed ingen genetisk uppgift. Den är däremot en biometrisk uppgift, eftersom det är möjligt att med hjälp av den unikt identifiera en person.

Mottagare

I 3 § personuppgiftslagen, som genomförde artikel 2 g i 1995 års dataskyddsdirektiv, anges att en myndighet inte ska anses som mottagare när personuppgifter lämnas ut till myndigheten för att den ska kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta. Vilka myndighetsuppdrag som avses kommenteras inte i förarbetena, utan där anges endast att definitionen av mottagare är avsedd att ha samma innebörd som motsvarande uttryck i direktivet (Personuppgiftslag, prop. 1997/98:44, s. 116). Ett motsvarande undantag har ansetts behövas i brottsdatalagen (prop. 2017/18:232 s. 89). Mottagare definieras därför i brottsdatalagen som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Definitionen bör användas även i den nya lagen.

Personuppgift

Personuppgifter är enligt brottsdatalagen varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. En motsvarande definition bör tas in i den nya lagen.

All information som kan hänföras till en fysisk person är en personuppgift. Det gäller även information som kan hänföras till en individ om en fysisk person kan identifieras med hjälp av informationen. Det krävs inte att den personuppgiftsansvarige ska förfoga över samtliga uppgifter som gör identifieringen möjlig. Det innebär att t.ex. oidentifierade fingeravtryck och dna-profiler är personuppgifter, eftersom det är möjligt att identifiera en person med hjälp av dem. Även bild- eller ljudupptagningar kan utgöra personuppgifter, om man direkt eller indirekt kan avgöra vilken individ som upptagningen avser. Uppgifter om avlidna personer omfattas inte av definitionen.

Registrerad

I brottsdatalagen avses med registrerad den fysiska person som personuppgiften gäller. En motsvarande definition bör tas in i den nya lagen.

Uppgift som rör hälsa

Varken 1995 års dataskyddsdirektiv eller personuppgiftslagen definierade vad som avses med uppgift om hälsa. I brottsdatalagen definieras uttrycket som en personuppgift som rör en persons fysiska eller psykiska hälsa,

inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus. En motsvarande definition bör tas in i den nya lagen.

7.8 Uppgifter om juridiska personer

Regeringens förslag: Lagen ska i viss utsträckning tillämpas vid behandling av uppgifter om juridiska personer.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt i denna del.

Skälen för regeringens förslag: I 1 kap. 6 § polisdatalagen föreskrivs att vissa bestämmelser i lagen även ska tillämpas på uppgifter om juridiska personer. För Säkerhetspolisens del gäller det bestämmelserna om ändamålen med behandlingen, tillgången till personuppgifter, bevarande och gallring och gemensamt tillgängliga uppgifter. Vid den översyn av registerförfattningarna som gjorts med anledning av införandet av brottsdatalagen har bestämmelser om skydd för uppgifter om juridiska personer behållits (prop. 2017/18:269 s. 112 f.). Regeringen anser att det bör gälla även för Säkerhetspolisen och en motsvarande reglering bör därför tas in i den nya lagen.

8 Rättslig grund och ändamål för behandlingen av personuppgifter

8.1 Skillnad mellan ändamålsbestämmelser och bestämmelser om rättslig grund

En grundläggande princip för all personuppgiftsbehandling är att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Principen kommer i dag till uttryck i både dataskyddsförordningen och brottsdatalagen (2018:1177). Både förordningen och lagen utgår också från att varje behandling av personuppgifter måste vila på en rättslig grund för att vara laglig. Det är alltså endast om det finns en rättslig grund som personuppgifter överhuvudtaget får behandlas. Kravet är inte nytt utan framgår av artikel 7 i 1995 års dataskyddsdirektiv och kom till uttryck i bl.a. 10 § personuppgiftslagen (1998:204). Det fördes dock inga resonemang kring kravet på rättslig grund i förarbetena till de registerförfattningar som tidigare gällde för de brottsbekämpande myndigheterna. I förarbetena till brottsdatalagen tog regeringen därför upp frågan om hur kravet på rättslig grund förhöll sig till de s.k. primära och sekundära ändamålsbestämmelserna i registerförfattningarna.

Regeringen konstaterade med hänvisning till Informationshanteringsutredningen att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser

ibland har blandats samman (SOU 2015:39 s. 277 f.). Det kan leda till att tillämparen förväxlar ändamål med rättslig grund och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål i det enskilda fallet. Det borde därför göras tydligare skillnad mellan bestämmelser om rättslig grund och ändamålsbestämmelser (Brottsdatalag, prop. 2017/18:232, s. 115). I myndigheternas registerförfattningar på brottsdatalagens område ersattes därefter de primära ändamålsbestämmelserna med bestämmelser om rättslig grund, se t.ex. 2 kap. 1 § polisens brottsdatalag, som ersatte 2 kap. 7 § polisdatalagen (2010:361).

I detta kapitel diskuteras först hur man bör se på ändamålsbestämmelserna i 6 kap. 1 och 2 §§ polisdatalagen (avsnitt 8.2). Hur regleringen bör utformas diskuteras i avsnitt 8.3 och hur ändamålen för behandling av personuppgifter ska bestämmas finns i avsnitt 8.4.

8.2 Dagens primära ändamålsbestämmelser är bestämmelser om rättslig grund

Regeringens bedömning: Det som i dag kallas primära ändamåls–bestämmelser är en del av den rättsliga grunden för behandling av personuppgifter. Det som kallas sekundära ändamålsbestämmelser bör dock fortfarande anses vara ändamålsbestämmelser. Regleringen bör ha i huvudsak samma innehåll som i dag.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen föreslår att även det som i dag kallas sekundära ändamålsbestämmelser ska vara en del av den rättsliga grunden för behandlingen av personuppgifter.

Remissinstanserna: Endast *Säkerhetspolisen* yttrar sig i denna del och anser att 6 kap. 1 polisdatalagen är tillräckligt preciserad för att utgöra en ändamålsbestämmelse och att det därför saknas skäl att ändra den gällande ordningen.

Skälen för regeringens bedömning

Dagens reglering

I 6 kap. 1 och 2 §§ polisdatalagen föreskrivs för vilka ändamål Säkerhetspolisen får behandla personuppgifter i sin brottsbekämpande verksamhet. Ändamålen delas upp i primära och sekundära. De primära ändamålen reglerar behandlingen av de personuppgifter som behövs i Säkerhetspolisens egen brottsbekämpande verksamhet. Myndigheten får t.ex. behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar bl.a. brott mot rikets säkerhet och terroristbrott. De sekundära ändamålen reglerar i vilken utsträckning personuppgifter som behandlas för något av de primära ändamålen får behandlas för att lämnas ut till andra för att tillgodose deras behov. Säkerhetspolisen får t.ex. behandla redan insamlade uppgifter när det är

nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos vissa andra myndigheter.

Primära ändamålsbestämmelser är bestämmelser om rättslig grund

Som framgår i avsnitt 8.1 anser regeringen att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. Det kan leda till att tillämparen förväxlar ändamål med rättslig grund och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål i det enskilda fallet. Det bör därför göras tydligare skillnad mellan bestämmelser om rättslig grund och ändamålsbestämmelser.

I avsnitt 8.4.1 föreslås att all behandling av personuppgifter även i fortsättningen ska utföras för särskilda, uttryckligt angivna och berättigade ändamål. Det är i förhållande till ändamålen som det ska prövas vilka personuppgifter som är adekvata och relevanta för behandlingen och att inte för många personuppgifter behandlas. Prövningen av att personuppgifter inte behandlas under längre tid än nödvändigt ska också ske i förhållande till ändamålen (avsnitt 12.2.1). Ändamålen måste därmed vara tillräckligt specifika för att ge ledning för dessa bedömningar. Mot den bakgrunden ansåg regeringen i förarbetena till brottsdatalagen att de primära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar borde ses som bestämmelser om rättslig grund. Bestämmelserna tydliggör att personuppgiftsbehandling är tillåten när uppgifterna fullgörs (prop. 2017/18:232 s. 123 f.). Frågan är om samma bedömning bör göras beträffande de primära och sekundära ändamålsbestämmelserna i 6 kap. 1 och 2 §§ polisdatalagen. *Säkerhetspolisen* har invänt att 6 kap. 1 § polisdatalagen är tillräckligt preciserad för att utgöra en ändamålsbestämmelse och att det därför saknas skäl att ändra gällande ordning.

Regleringen i 6 kap. 1 § polisdatalagen är delvis annorlunda utformad än de tidigare primära ändamålsbestämmelserna i t.ex. 2 kap. 7 § polisdatalagen. Paragrafen är mer detaljerad. Det beror framför allt på att Säkerhetspolisen har ett betydligt mer begränsat uppdrag än exempelvis Polismyndigheten. Som utredningen framhåller ger dock paragrafen inte någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. Det anges endast att Säkerhetspolisen får behandla personuppgifter för att utföra vissa av sina arbetsuppgifter. Syftet är att precisera när personuppgifter alls får behandlas i Säkerhetspolisens brottsbekämpande verksamhet. Paragrafen utgör därmed den yttre ram inom vilken de särskilda, uttryckligt angivna och berättigade ändamålen med behandlingen i enskilda fall ska bestämmas. Regeringen delar mot den bakgrunden utredningens bedömning att de primära ändamålsbestämmelserna i 6 kap. 1 § polisdatalagen inte är ändamålsbestämmelser i egentlig mening, utan en del av den rättsliga grunden. Vad *Säkerhetspolisen* anfört i denna del föranleder ingen annan bedömning.

När det gäller de sekundära ändamålsbestämmelserna i 6 kap. 2 § polisdatalagen är situationen en annan än för de primära ändamålsbestämmelserna i 6 kap. 1 §. De sekundära ändamålsbestämmelserna

anger endast i vilken utsträckning som Säkerhetspolisen får lämna personuppgifter till andra och förutsätter att det redan finns stöd för behandlingen enligt 1 §. Det är alltså inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem med stöd av 2 §. Vidare innehåller paragrafen en uppräkning av flera förhållandevis specifika situationer. Mot den bakgrunden anser regeringen, till skillnad från utredningen, att de nuvarande sekundära ändamålsbestämmelserna inte kan ses som en del av den rättsliga grunden för behandling av personuppgifter. Den rättsliga grunden finns även i dessa situationer angiven i 1 §. Systematiken i lagen kommer då också att i högre grad motsvara systematiken på brottsdatalagens område, där det endast finns mer allmänt hållna bestämmelser om rättslig grund (se t.ex. 2 kap. 1 § brottsdatalagen och 2 kap. 1 § polisens brottsdatalag). Regeringen instämmer dock i utredningens bedömning att regleringen bör i huvudsak ha samma sakliga innehåll som i dag, vilket utvecklas i avsnitt 8.4.3.

8.3 Rättslig grund för behandling

8.3.1 Rättslig grund för behandling – huvudregeln

Regeringens förslag: Personuppgifter ska få behandlas om det är nödvändigt för att Säkerhetspolisen ska kunna

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
   a) brott mot Sveriges säkerhet,
   b) terrorbrott, eller
   c) tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,
2. utreda eller lagföra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra uppgifter
   a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
   b) enligt säkerhetsskyddslagen (2018:585), eller
   c) enligt utlännings- och medborgarskapslagstiftningen,
4. fullgöra annan uppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen, eller
5. fullgöra förpliktelser som följer av internationella åtaganden.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår också att det i lagen uttryckligen ska anges att uppgiften ska framgå av lag, förordning eller av ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

Remissinstanserna: Endast *Säkerhetspolisen* uttalar sig i denna del och anser att rekvisitet nödvändigt ska ersättas med behövs som i 6 kap. 1 § polisdatalagen.

Skälen för regeringens förslag

En bestämmelse om rättsliga grunder behövs

Som framgår av avsnitt 8.1 utgår både dataskyddsdirektivet och dataskyddsförordningen från att varje behandling måste vila på en rättslig grund för att vara laglig. I artikel 6.1 i förordningen finns det en uttömmande uppräkning av de rättsliga grunderna för behandling av personuppgifter enligt förordningen. Någon motsvarande uppräkning finns inte i direktivet. Däremot anges förutsättningarna för att en behandling ska vara laglig i artikel 8.1.

Brottsdatalagen innehåller bestämmelser om rättsliga grunder. Enligt 2 kap. 1 § får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Uppgiften ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften (prop. 2017/18:232 s. 116–118). För att personuppgiftsbehandling ska vara tillåten enligt brottsdatalagen krävs det således både en reglerad arbetsuppgift och bestämmelser om att personuppgifter får behandlas för att utföra uppgiften. Detsamma bör gälla för Säkerhetspolisen. Regeringen delar därför utredningens bedömning att det bör finnas en bestämmelse i den nya lagen som anger de rättsliga grunderna för personuppgiftsbehandlingen.

Utformningen av bestämmelsen

Regleringen i 6 kap. 1 § polisdatalagen korresponderar i princip med 3 § polislagen (1984:387) som anger Säkerhetspolisens huvudsakliga uppgifter. Bestämmelsen har endast förändrats marginellt sedan polisdatalagens tillkomst. Den bedömning av Säkerhetspolisens behov av att behandla personuppgifter som gjordes då gör sig fortfarande gällande (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 255 f.). Den nya lagen bör i huvudsak innehålla samma reglering.

Utredningen föreslår att det särskilt ska anges att uppgifterna ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften. Att ett sådant krav infördes i brottsdatalagen var en följd av regleringen i dataskyddsdirektivet. En förutsättning för att Säkerhetspolisen ska få behandla personuppgifter är att Säkerhetspolisens har ålagts att utföra en viss arbetsuppgift. Vilka arbetsuppgifter Säkerhetspolisen har framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften. Ett motsvarande krav behöver därför inte särskilt anges i förevarande paragraf.

Säkerhetspolisen förespråkar att ordet ”behövs” används i lagtexten för att det inte ska framstå som att kravet för att få behandla personuppgifter har höjts. Eftersom ”nödvändigt” är det ord som finns i artikeln om rättslig grund i dataskyddsförordningen valdes det ordet även i brottsdatalagens bestämmelse om rättslig grund. Även om det inte finns något som hindrar att den nya lagen i detta avseende utformas på annat sätt än brottsdatalagen anser regeringen att skälen för en enhetlig terminologi överväger. Samma uttryckssätt som i brottsdatalagen bör därför användas i den nya lagen.

Som anges i förarbetena till brottsdatalagen bör ordet ”nödvändigt” i detta sammanhang tolkas som att det är fråga om något som behövs för att på ett effektivt sätt kunna utföra uppgiften (prop. 2017/18:232 s. 117). Trots att terminologin ändras blir det därför inte fråga om någon ändring i förhållande till vad som krävs enligt dagens reglering.

Enligt 6 kap. 1 § 5 polisdatalagen får Säkerhetspolisen behandla personuppgifter om det behövs för att lämna tekniskt biträde till vissa andra brottsbekämpande myndigheter. Den uppgiften omfattas i dag av brottsdatalagens tillämpningsområde (prop. 2017/18:232 s. 105). Personuppgiftsbehandling för sådant biträde bör därför inte regleras i den nya lagen.

Uppgifter enligt utlännings- och medborgarskapslagstiftningen

Säkerhetspolisen har vissa uppgifter enligt utlännings- och medborgarskapslagstiftningen (avsnitt 4.1). Det framgår inte av förarbetena till polisdatalagen hur lagstiftaren ser på personuppgiftsbehandling för sådana ändamål.

I förarbetena till utlänningsdatalagen (2016:27) konstaterar regeringen att all verksamhet hos Säkerhetspolisen i någon mening är brottsbekämpande. Mot den bakgrunden och då Säkerhetspolisens uppgifter på utlännings- och medborgarskapsområdet är förhållandevis begränsade ansågs det inte vara ändamålsenligt att låta Säkerhetspolisen omfattas av utlänningsdatalagens reglering. Konsekvensen blev att Säkerhetspolisen i stället antingen ska tillämpa de särskilda regler om personuppgiftsbehandling som gäller för myndigheten enligt polisdatalagen eller personuppgiftslagen (Utlänningsdatalag, prop. 2015/16:65, s. 40). Mot bakgrund av förarbetsuttalandena och att personuppgiftslagen har upphävts är det nödvändigt att reglera myndighetens personuppgiftsbehandling på området.

Säkerhetspolisens arbetsuppgifter enligt utlännings- och medborgarskapslagstiftningen syftar till att förhindra att individer som är eller kan bli ett säkerhetshot mot Sverige etablerar sig i landet. Utifrån vad som är känt om personens bakgrund, kontakter eller egna aktiviteter gör Säkerhetspolisen en bedömning av om han eller hon kan komma att ägna sig åt säkerhetshotande verksamhet. Säkerhetsskälen kan exempelvis bestå av kopplingar till personer som antas syssla med olovlig underrättelseverksamhet eller terrorism. Mot den bakgrunden anser regeringen, i likhet med utredningen, att Säkerhetspolisens uppgifter enligt utlännings- och medborgarskapslagstiftningen är ett led i uppgifterna som rör nationell säkerhet och därför bör anges som en tillåten rättslig grund för behandling av personuppgifter i den nya lagen.

8.3.2 Rättslig grund i undantagsfall för diarieföring och handläggning

Regeringens förslag: Personuppgifter ska få behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Säkerhetspolisen tar dagligen emot stora mängder information, ofta i elektronisk form. De inkommande uppgifterna kan vara en del av en allmän handling i tryckfrihetsförordningens mening. Enligt 5 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska som huvudregel allmänna handlingar som kommit in till en myndighet registreras, dvs. diarieföras, så snart som möjligt. En myndighet måste därför alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande handlingar. Det gäller även i de fall där myndigheten inte behöver behandla personuppgifterna för att utföra sina uppgifter (prop. 2009/10:85 s. 112 f.) I 6 kap. 3 § polisdatalagen föreskrivs att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Det bör tas in en motsvarande bestämmelse i den nya lagen som tydliggör att det är en tillåten rättslig grund för behandling.

8.4 Ändamål för behandling

8.4.1 Behandling bara för särskilda, uttryckligt angivna och berättigade ändamål

Regeringens förslag: Säkerhetspolisen ska få behandla personuppgifter bara för särskilda, uttryckligt angivna och berättigade ändamål.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna Endast *Säkerhetspolisen* yttrar sig i denna del och anför att om 6 kap. 1 § polisdatalagen är att anse som en bestämmelse om rättslig grund och inte en ändamålsbestämmelse, måste det i det fortsatta lagstiftningsarbetet klarläggas hur ändamålen ska utformas.

Skälen för regeringens förslag: I 9 § första stycket c personuppgiftslagen finns det grundläggande kravet på att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Kravet gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen. Det är dock inte bara när personuppgifter samlas in som det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen. I brottsdatalagen har det tydliggjorts genom att det i 2 kap. 3 § föreskrivs att all behandling ska utföras för särskilda, uttryckligt angivna och berättigade ändamål (prop. 2017/18:232 s. 120–122). En motsvarande bestämmelse bör tas in i den nya lagen.

Att ändamålen ska vara särskilda innebär att de måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska kunna avgöras att inte för många uppgifter behandlas (avsnitt 9.1.4). Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Ändamålen ska anges uttryckligen redan när personuppgifterna samlas in.

Att ändamålen ska vara berättigade innebär en koppling till den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som

inte är berättigat i förhållande till den tillämpliga rättsliga grunden. Kravet på att ändamålet för behandlingen ska vara berättigat kan också sägas innebära ett krav på att behandlingen ska vara förenlig med konstitutionella och andra rättsliga principer.

En särskild fråga är vad som avses med att ändamålen ska vara uttryckligt angivna. Regeringen återkommer till den frågan i samband med att frågan om att ändamålen i vissa fall ska framgå genom en särskild upplysning behandlas (avsnitt 10.2).

Säkerhetspolisen anför att det måste klarläggas hur ändamålen ska utformas om de primära ändamålsbestämmelserna är att anse som bestämmelser om rättslig grund (jfr avsnitt 8.2). En mycket stor del av den information som Säkerhetspolisen behandlar är underrättelseinformation. I underrättelseverksamhet, där personuppgifter behandlas på ett tidigt stadium i processen, är det långtifrån alltid möjligt att ange ändamålen för behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. I Säkerhetspolisens verksamhet går det exempelvis inte att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet som i annan brottsbekämpande verksamhet. Det innebär att ändamålet kanske till en början inte kan anges mer preciserat än till vilken verksamhetsområde en viss uppgift hör, exempelvis kontraterrorism. Å andra sidan är Säkerhetspolisens verksamhet inriktad mot ett fåtal väl avgränsade företeelser som är av särskilt samhällsfarlig karaktär (prop. 2009/10:85 s. 256). Det får därför accepteras att beskrivningen av ändamålen inte alltid kan ha samma precision som i annan brottsbekämpande verksamhet. Det finns vidare inget som hindrar att det närmare ändamålet med behandlingen inledningsvis är detsamma som anges i bestämmelsen om rättslig grund. Ändamålet får sedan preciseras mer när det blir möjligt. Att det som i dag kallas primära ändamålsbestämmelser i stället ses som bestämmelser om rättslig grund ska alltså inte påverka hur Säkerhetspolisen bestämmer ändamålen för behandlingen av personuppgifter.

8.4.2 Allmänt om behandling för nya ändamål

Regeringens förslag: Personuppgifter ska inte få behandlas för något ändamål som är oförenligt med det ändamål personuppgifterna ursprungligen behandlades för.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 9 § första stycket d personuppgiftslagen finns en generell bestämmelse om behandling för nya ändamål. Där regleras finalitetsprincipen, enligt vilken personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen.

I 2 kap. 4 § brottsdatalagen föreskrivs att det, innan personuppgifter får behandlas för ett nytt ändamål inom lagens tillämpningsområde, ska säkerställas att det finns en tillåten rättslig grund för den nya behandlingen och att behandlingen är nödvändig och proportionerlig för det nya

ändamålet. Att en sådan bedömning ska göras vid behandling för nya ändamål inom brottsdatalagens tillämpningsområde framgår av artikel 4.2 i dataskyddsdirektivet. Finalitetsprincipen regleras emellertid också i direktivet. I artikel 4.1 b anges att personuppgifter inte får behandlas på ett sätt som står i strid med de ändamål som uppgifterna samlades in för. I förarbetena till brottsdatalagen görs bedömningen att all behandling för ändamål inom direktivets tillämpningsområde ska anses vara förenlig med insamlingsändamålen, under förutsättning att behandlingen är nödvändig och står i proportion till det nya ändamålet. Någon prövning mot det ursprungliga ändamålet behöver således inte göras vid behandling för nya ändamål inom brottsdatalagens tillämpningsområde. Eftersom bestämmelserna i dataskyddsförordningen ska tillämpas vid behandling för ändamål utanför brottsdatalagens tillämpningsområde ska någon prövning mot det ursprungliga ändamålet inte göras då heller. Det beror på att den behandlingen blir den första behandlingen enligt förordningen och att det därför inte är fråga om någon behandling för nya ändamål där finalitetsprincipen ska tillämpas (prop. 2017/18:232 s. 126 och 132). Finalitetsprincipen regleras därför inte i brottsdatalagen.

Säkerhetspolisen behöver i likhet med andra brottsbekämpande myndigheter kunna behandla personuppgifter för nya ändamål, t.ex. använda information från en förundersökning för att förebygga nya brott. Frågan är om prövningen enligt finalitetsprincipen bör ersättas av samma prövning av nödvändighet och proportionalitet som för övriga brottsbekämpande myndigheter.

Kraven på nödvändighet och proportionalitet i brottsdatalagen har sin grund i direktivet. Direktivets krav gäller dock inte på den nya lagens område eftersom behandling av personuppgifter som rör nationell säkerhet undantas från direktivets tillämpningsområde. Det finns därför inget som hindrar att en reglering som bygger på finalitetsprincipen väljs för Säkerhetspolisen. Regeringen anser i likhet med utredningen att det med tanke på Säkerhetspolisens uppdrag finns fördelar med att behålla den inarbetade ordningen. Finalitetsprincipen bör därför fortsätta att gälla för Säkerhetspolisens behandling av personuppgifter för nya ändamål.

När Säkerhetspolisen ska behandla personuppgifter för nya ändamål bör myndigheten alltid pröva om det nya ändamålet är förenligt med det ändamål som personuppgifterna samlades in för. Eftersom verksamheten är inriktad på att bekämpa brott som är systemhotande kan Säkerhetspolisens behandling av personuppgifter för nya ändamål för den egna verksamheten i de allra flesta fall anses förenlig med ursprungsändamålet. Vad som bör gälla när myndigheten behandlar personuppgifter för att tillhandahålla information som behövs i annan verksamhet tas upp i avsnitt 8.4.3.

8.4.3 Behandling för ändamål i annan verksamhet

Regeringens förslag: Personuppgifter som Säkerhetspolisen behandlar ska även få behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet hos Polismyndigheten,

Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,

3. i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelseverksamhet, om det finns särskilda skäl att tillhandahålla informationen,

4. i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med en viss uppgift,

5. i brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller

6. i verksamhet hos en utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter ska även få behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen och till andra, om skyldighet att lämna uppgifter följer av lag eller förordning.

I ett enskilt fall ska personuppgifter få behandlas för att tillhandahålla information för något annat ändamål än de ovan uppräknade, om det nya ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen anser dock att de aktuella bestämmelserna är bestämmelser om rättslig grund och inte ändamålsbestämmelser.

Remissinstanserna: *Datainspektionen* avstyrker utredningens förslag att ge Säkerhetspolisen möjlighet att tillhandahålla information till Försvarets radioanstalt då inspektionen anser att det inte konstaterats om det finns ett behov av informationsutbytet. Övriga remissinstanser uttalar sig inte i denna del.

Skälen för regeringens förslag: Regeringen bedömer att bestämmelserna i 6 kap 2 § polisdatalagen återspeglar Säkerhetspolisens behov av att behandla personuppgifter för att tillgodose andras informationsbehov. De skäl som anfördes när regleringen infördes gör sig fortfarande gällande (prop. 2009/10:85, s. 260 f. och Den nya polisorganisationen – några frågor om personuppgiftsbehandling m.m., prop. 2014/15:94 s. 83 f.). Den nya lagen bör därför i huvudsak ha samma innehåll. Av de skäl som anges i avsnitt 8.2 anser regeringen, till skillnad från utredningen, att bestämmelserna är ändamålsbestämmelser och inte bestämmelser om rättslig grund.

Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt har angränsande uppdrag beträffande Sveriges säkerhet som förutsätter nära samarbete och kontinuerligt informationsutbyte. På samma sätt som brottsbekämpning i vissa avseenden är en för flera myndigheter gemensam angelägenhet är också underrättelseverksamhet som rör Sveriges säkerhet en för Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt gemensam angelägenhet, även om myndigheterna har olika uppdrag i förhållande till Sveriges säkerhet. Det måste därför, som föreslås av utredningen, finnas ett utrymme för att utbyta information mellan myndigheterna. Även om Säkerhetspolisen i de flesta fall lämnar information till Försvarets radioanstalt för den egna verksamhetens behov, kan Försvarets radioanstalt behöva sådan information för sin egen

verksamhet. Regeringen anser därför i likhet med utredningen, men till skillnad från *Datainspektionen*, att det bör finnas rättsligt stöd även för ett sådant utlämnande. Av samma anledning som när det gäller information till Försvarsmakten bör det krävas särskilda skäl för att Säkerhetspolisen ska få lämna ut uppgifterna (prop. 2009/10:85 s. 262). Härigenom markeras att bestämmelsen ska tillämpas restriktivt. Försvarets radioanstalt bör därför läggas till i bestämmelsen som reglerar utlämnande till Försvarsmakten.

Enligt 16 § förordningen (2014:1103) med instruktion för Säkerhetspolisen ska myndigheten samarbeta med utländska myndigheter och organ i den utsträckning som behövs för myndighetens verksamhet och som regeringen närmare bestämmer. Säkerhetspolisen har flera utländska samarbetspartner och utbyter kontinuerligt information med dem. I avsnitt 11.3.3 föreslås att Säkerhetspolisen ska kunna medge underrättelse- och säkerhetstjänster i EU och EES direktåtkomst till vissa uppgifter. Även om Säkerhetspolisen i de flesta fall lämnar informationen till dem för den egna verksamhetens behov, kan det inte uteslutas att Säkerhetspolisen även kan behöva lämna information för att tillgodose de utländska tjänsternas behov. Det kan t.ex. gälla misstanke om ett förestående attentat som uteslutande berör en annan stat. I 6 kap. 2 § polisdatalagen anges endast brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation som mottagare. Utländska underrättelse- och säkerhetstjänster har inte alltid den uppgiften. För att det ska vara tydligt att Säkerhetspolisen får lämna information om det behövs för sådana tjänsters behov bör det införas rättsligt stöd för det.

8.4.4 Behandling för vetenskapliga, statistiska och historiska ändamål

Regeringens förslag: Säkerhetspolisen ska få behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom den nya lagens tillämpningsområde.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 9 § andra stycket personuppgiftslagen ska behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte anses oförenlig med de ändamål för vilka personuppgifterna samlades in. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen och innebär att personuppgifter som regel får behandlas för sådana ändamål.

I 2 kap. 5 § brottsdatalagen föreskrivs att en behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Genom att det lyfts fram att behandling av personuppgifter kan inbegripa vetenskaplig, statistisk eller historisk användning blir det tydligt att lagens övriga bestämmelser ska tillämpas även vid behandling för sådana ändamål (prop. 2017/18:232 s. 139). Behandling för vetenskapliga, statistiska och historiska ändamål

bör vara tillåten även enligt den nya lagen. Bestämmelsen bör formuleras på samma sätt som motsvarande bestämmelse i brottsdatalagen.

9 Behandling av personuppgifter

9.1 Grundläggande krav på behandlingen

9.1.1 Krav på författningsenlig och korrekt behandling

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

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för utredningens förslag: I 9 § personuppgiftslagen regleras de grundläggande principerna för personuppgiftsbehandling. I brottsdatalagen (2018:1177) har de grundläggande principerna i stället delats upp och behandlas tillsammans med regleringen av de frågor som respektive princip tar sikte på (Brottsdatalag, prop. 2017/18:232, s. 141 f.). Samma lösning bör väljas i den nya lagen.

Enligt 9 § första stycket a och b personuppgiftslagen (1998:204) får personuppgifter behandlas bara om det är lagligt. Personuppgifterna ska vidare behandlas på ett korrekt sätt och i enlighet med god sed. Bestämmelserna gäller genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen (2010:361) för Säkerhetspolisen. Att en myndighet ska agera i enlighet med lag framstår som en självklarhet och är djupt förankrat i den svenska förvaltningstraditionen. Det gäller också att handläggningen ska ske på ett korrekt sätt. Det bör emellertid tydliggöras i den nya lagen att personuppgifter alltid ska behandlas lagligt och på ett korrekt sätt.

I 2 kap. 6 § brottsdatalagen föreskrivs att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt. Skälet till att ordet författningsenlig används i stället för laglig är enligt förarbetena att ordet laglig lätt kan leda till motsatsslut och att det i andra bestämmelser i lagen regleras att behandlingen ska stå i överensstämmelse inte bara med lag utan även med föreskrifter på lägre nivåer (prop. 2017/18:232 s. 142 f.). Samma överväganden gör sig gällande i förhållande till Säkerhetspolisen och en motsvarande bestämmelse bör tas in även i den nya lagen.

Att personuppgifter ska behandlas författningsenligt innebär att det ska finnas en rättslig grund för behandlingen (avsnitt 8.3.1). Att personuppgifterna ska behandlas korrekt innefattar att behandlingen inte bara formellt ska vara i enlighet med regleringen utan också spegla intentionerna med lagstiftningen.

9.1.2 Personuppgifter ska vara korrekta, adekvata och relevanta

Regeringens förslag: De personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

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

De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Utredningens förslag överensstämmer med regeringens förslag.

Remissinstanserna: Endast *Datainspektionen* yttrar sig i denna del. Inspektionen ifrågasätter inte att det kan finnas ett mycket kortvarigt behov för Säkerhetspolisen att vid informationsinhämtning behandla uppgifter om andra än den misstänkte för att inte avslöja vem misstanken riktas mot och anser att de uppgifter som behandlas då kan anses både adekvata och relevanta under insamlingsfasen. Det måste dock ställas högre krav på insamlingen av uppgifter om andra än den misstänkte och de bör skyddas av särskilda skyddsåtgärder, t.ex. genom krav på särskilda beslutsfattare och att det garanteras att informationen raderas omgående efter att Säkerhetspolisen samlat in den.

Skälen för regeringens förslag

Personuppgifter ska vara korrekta och uppdaterade

Enligt 9 § första stycket g personuppgiftslagen ska personuppgifter som behandlas vara riktiga och, om nödvändigt, aktuella. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen. I 2 kap. 7 § första stycket brottsdatalagen finns en bestämmelse med motsvarande innehåll, men den har formulerats något annorlunda. Personuppgifter som behandlas ska enligt bestämmelsen vara korrekta och, om det är nödvändigt, uppdaterade. En motsvarande bestämmelse bör tas in i den nya lagen.

En uppgift är korrekt om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är som personuppgifterna ska spegla får man söka ledning i ändamålen med behandlingen. I vissa fall är avsikten med behandlingen bara att registrera uppgifter som kommit in, t.ex. i en brottsanmälan. De behandlade personuppgifterna får då betraktas som korrekta om de stämmer överens med de inkomna uppgifterna, oavsett hur de förhåller sig till de verkliga förhållandena (jfr Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen, En kommentar, 4:e uppl. 2011, i fortsättningen Öman m.fl., s. 206).

Bedömningen av om en personuppgift är korrekt ska inte bara utgå från ändamålen för behandlingen. Att uppgifter som förekommer i bl.a. brottsbekämpande verksamhet och vid annan behandling av uppgifter om lagöverträdelser har en särskild karaktär måste också beaktas. Frågan om en uppgift är korrekt måste därför även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. Om t.ex. en person anmäler

en annan för brott är uppgifterna i anmälan korrekta om de återspeglar vad anmälaren har uppgett. Det förhållandet att det senare hålls ett förhör vid vilket vissa uppgifter tas tillbaka eller ändras innebär inte att de först nedtecknade uppgifterna i anmälan är felaktiga. Om det sedan vid en rättegång visar sig att personen i fråga lämnar nya uppgifter eller ändrar tidigare påståenden återspeglar ändå en uppteckning av tidigare förhör vad som sades vid det tillfället och är därigenom korrekt. Bedömningen blir densamma i underrättelseverksamheten, där en uppgift måste anses korrekt om den återger vad som inkommit i underrättelseflödet även om det senare visar sig att uppgiften inte stämmer överens med verkligheten.

De behandlade uppgifterna behöver bara vara uppdaterade om det är nödvändigt. Frågan om det är nödvändigt att uppgifterna är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen (jfr Öman m.fl. s. 206). Exempelvis kan adressuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras. När ärendet har avslutats är det dock inte nödvändigt att uppdatera en adressuppgift.

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

I 2 kap. 10 § tredje stycket polisdatalagen, som gäller för Säkerhetspolisen genom en hänvisning i 6 kap. 4 § 4, föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt och med respekt för människovärdet. En motsvarande bestämmelse bör tas in i den nya lagen.

Bestämmelsen finns i dag i den paragraf som reglerar användningen av känsliga personuppgifter. Regleringen har lett till viss osäkerhet om signalementsuppgifter är känsliga personuppgifter. I 2 kap. 7 § andra stycket brottsdatalagen har bestämmelsen därför placerats tillsammans med reglerna om personuppgifters kvalitet för att tydliggöra att uppgifter om utseende inte i sig ska betraktas som känsliga personuppgifter. Den lösningen bör väljas även i den nya lagen. Ett signalement kan dock innehålla uppgifter ur vilka man kan utläsa uppgifter om t.ex. hälsa eller etniskt ursprung. Sådana uppgifter ska hanteras enligt reglerna om känsliga personuppgifter (avsnitt 9.1.2).

Personuppgifter ska vara adekvata och relevanta

Enligt 9 § första stycket e och f personuppgiftslagen ska de personuppgifter som behandlas vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen. Motsvarande reglering finns i 2 kap. 8 § brottsdatalagen. En likadan bestämmelse bör tas in i den nya lagen.

Vilka uppgifter som är adekvata och relevanta ska bedömas i förhållande till ändamålen med behandlingen. Detsamma gäller hur många personuppgifter det finns behov av att behandla. Det kan emellertid vara svårare att bedöma om uppgifterna är adekvata och relevanta i Säkerhetspolisens verksamhet än i annan polisverksamhet, eftersom det som regel inte är lika tydligt vari den brottsliga verksamheten eller säkerhetshotet består.

Att det krävs att uppgifterna ska vara adekvata och relevanta får betydelse för hur s.k. överskottsinformation ska hanteras, dvs. uppgifter som samlas in och som visar sig inte vara adekvata eller relevanta för det bestämda ändamålet. Om uppgifterna inte behövs för något annat tillåtet ändamål får de inte lagras för framtida behov. Det finns särskilda regler om i vilken utsträckning överskottsinformation överhuvudtaget får behandlas i vissa sammanhang (t.ex. 27 kap. 23 a § rättegångsbalken).

Med hänsyn till Säkerhetspolisens känsliga verksamhet kan det, bl.a. vid bedömningen av hur många personuppgifter som behöver behandlas i förhållande till ändamålet, vara nödvändigt att utöver behoven i det konkreta ärendet ta hänsyn till andra aspekter, framför allt hur säkra de system som Säkerhetspolisen har direktåtkomst till är. Säkerhetspolisen kan t.ex. i vissa situationer behöva begära uppgifter om fler personer än den som är misstänkt för att inte avslöja vem eller vilka personer som myndigheten intresserar sig för i sitt underrättelsearbete eller i en brottsutredning. Regeringen delar utredningens bedömning att kravet på att uppgifterna ska vara adekvata och relevanta och inte för många i förhållande till ändamålet med behandlingen ändå bör anses vara uppfyllt vid själva sökningen. Behovet av att behandla sådana uppgifter är mycket kortvarigt och ska givetvis upphöra så snart syftet med sökningen är uppnått. Regeringen anser därför, till skillnad från *Datainspektionen*, att det inte finns skäl att förena den här typen av sökningar med några särskilda krav på skyddsåtgärder.

Särskilt om material från användning av hemliga tvångsmedel

Säkerhetspolisen behandlar i stor utsträckning material som inhämtats genom hemliga tvångsmedel. Det beror dels på att Säkerhetspolisen biträder andra brottsbekämpande myndigheter med tekniska åtgärder, dels på att sådana tvångsmedel förekommer i Säkerhetspolisens egen verksamhet. För behandling av uppgifter som inhämtas genom hemliga tvångsmedel gäller dels reglerna i rättegångsbalken eller motsvarande lagstiftning, dels myndighetens registerlagstiftning (Integritet och effektivitet i polisen brottsbekämpande verksamhet, prop. 2009/10:85, s. 78). Material av nu aktuellt slag kan både behöva bearbetas tekniskt eller på annat sätt, och i vissa fall även tolkas eller översättas, innan det kan granskas på det sätt som förutsätts i rättegångsbalken och annan motsvarande lagstiftning. Det ligger i sakens natur att kravet på granskning av det materiella innehållet inte kan uppfyllas innan det har gjorts tillgängligt på sådant sätt att en åklagare eller den utredningspersonal som biträder honom eller henne kan ta del av det. Det innebär att personuppgifter måste kunna behandlas för att den granskningen ska kunna komma till stånd. Kravet på att sådant material som härrör från hemliga tvångsmedel och som är ovidkommande ska tas bort så snabbt som möjligt måste därför ses i ljuset av möjligheterna att på ett tidigt stadium kunna bedöma värdet av informationen.

9.2 Känsliga personuppgifter

9.2.1 Känsliga personuppgifter får behandlas i samma utsträckning som i dag

Regeringens förslag: Säkerhetspolisen ska inte få behandla personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning. Om uppgifter om en person behandlas ska de dock få kompletteras med sådana uppgifter när det är absolut nödvändigt för ändamålet med behandlingen.

Säkerhetspolisen ska få behandla biometriska uppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen, men ska inte få behandla genetiska uppgifter.

Känsliga personuppgifter får alltid behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* påpekar att 2 kap. 10 § i den nya lagen inte helt överensstämmer med motsvarande bestämmelse i förslaget till brottsdatalag. *Säkerhetspolisen* framhåller att myndigheten har ett faktiskt behov av att kunna samla in dna-spår och att kunna ta emot genetiska uppgifter som ges in till myndigheten, exempelvis från samarbetspartner. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Fler kategorier av uppgifter blir känsliga personuppgifter

Enligt 2 kap. 10 § polisdatalagen, som genom en hänvisning i 6 kap. 4 § 4 gäller för Säkerhetspolisen, får uppgifter om en person 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 redan behandlas på någon annan grund, får de dock kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Innebörden är att det t.ex. inte är tillåtet att föra särskilda register över personer baserat på deras politiska åsikter. Om uppgifter om en person redan behandlas får dock uppgifter om politiska åsikter behandlas, om det bedöms vara absolut nödvändigt för ändamålet med behandlingen. Det kan t.ex. vara fallet om motivet för ett brott är politiskt.

I brottsdatalagen utökas uppräkningen av vad som betecknas som känsliga personuppgifter. Dit hör enligt 2 kap. 11 § även uppgifter som rör sexuell läggning och enligt 2 kap. 12 § biometriska och genetiska uppgifter.

För att den nya regleringen så långt möjligt ska stämma överens med övriga registerförfattningar bör uppräkningen av känsliga personuppgifter i den nya lagen omfatta både uppgifter som rör sexualliv och sexuell läggning. Även biometriska och genetiska uppgifter bör i den nya lagen

betecknas som känsliga personuppgifter. Vad som avses med genetiska och biometriska uppgifter redovisas i avsnitt 7.7. I förarbetena till brottsdatalagen utvecklas varför ordet ”ras” även fortsättningsvis används (prop. 2017/18:232 s. 151 f.).

Känsliga personuppgifter bör få behandlas i samma utsträckning som i dag

På samma sätt som i dag bör Säkerhetspolisen bara få behandla känsliga personuppgifter om uppgifter om personen redan behandlas på någon annan grund och behandlingen av känsliga personuppgifter är absolut nödvändig för ändamålet med behandlingen. Bestämmelserna om känsliga personuppgifter i den nya lagen bör formuleras på samma sätt som i brottsdatalagen. Det blir då tydligare vilka uppgifter som utgör känsliga personuppgifter och när de får behandlas. Någon förändring av synen på vad som är absolut nödvändigt vid behandling av känsliga personuppgifter är inte avsedd. Sådana uppgifter ska alltjämt användas restriktivt och behovet av att komplettera med sådana uppgifter ska prövas noga i det enskilda ärendet (prop. 2009/10:85 s. 325). Säkerhetspolisens möjligheter att behandla sådana uppgifter som redan i dag betecknas som känsliga personuppgifter förändras därmed inte.

Behandling av biometriska och genetiska uppgifter

Fingeravtryck eller dna-spår från personer som inte förekommer i fingeravtrycks- eller dna-registren är vanligt förekommande i brottsbekämpande verksamhet. Sådana oidentifierade fingeravtryck eller dna-spår som genomgår särskild teknisk behandling för att möjliggöra unik identifiering utgör som framgår av avsnitt 7.7 biometriska uppgifter. Regeln om att känsliga personuppgifter endast får behandlas om någon annan uppgift om personen i fråga samtidigt behandlas fungerar därmed inte när det gäller oidentifierade avtryck eller spår. Behandlingen av biometriska och genetiska uppgifter regleras därför särskilt i brottsdatalagen (prop. 2017/18:232 s. 154). Enligt 2 kap. 12 § brottsdatalagen får biometriska och genetiska uppgifter behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

I förarbetena till de brottsbekämpande myndigheternas registerförfattningar konstaterar regeringen att Polismyndigheten och Säkerhetspolisen har behov av att behandla biometriska uppgifter (prop. 2017/18:269 s. 150 f.). Regeringen delar utredningens bedömning att detta gäller även när behandlingen rör nationell säkerhet. En bestämmelse motsvarande 2 kap. 12 § brottsdatalagen för biometriska uppgifter bör därför tas in i den nya lagen.

Genetiska uppgifter föreslogs enbart få behandlas i Polismyndighetens forensiska verksamhet (prop. 2017:18:269 s. 151 och 6 kap. 4 § polisens brottsdatalag). Utredningen föreslår att Säkerhetspolisen inte ska får behandla genetiska uppgifter, eftersom myndigheten inte behandlar sådana uppgifter i dag och det inte heller kan förutses något framtida behov av det. *Säkerhetspolisen* har invänt att myndigheten har ett faktiskt behov av att kunna samla in dna-spår och att kunna ta emot genetiska uppgifter som ges in till Säkerhetspolisen, exempelvis från myndighetens samarbetspartner. Med genetiska uppgifter avses enligt den definition som

föreslås i avsnitt 7.7 personuppgifter som rör en persons nedärvda eller förvärvade kännetecken som härrör från en analys av ett spår eller ett prov från personen. Det innebär att ett dna-spår eller ett dna-prov inte utgör genetiska uppgifter, utan det är enbart den information som kan tas fram ur spåret eller provet som utgör sådana uppgifter. Genetiska uppgifter behandlas vid dna-analyser i den forensiska verksamheten för att ta fram dna-profiler eller forensiska uppslag (prop. 2017/18:232 s. 435 f.). Säkerhetspolisen kan alltså säkra dna-spår och skicka eller ta emot dna-spår eller dna-profiler utan att myndigheten behandlar genetiska uppgifter. Själva dna-profilen är endast en sifferkombination och därmed ingen genetisk uppgift. Den är däremot en biometrisk uppgift som Säkerhetspolisen föreslås få rätt att behandla om det är absolut nödvändigt. Det har således inte framkommit att Säkerhetspolisen har något konkret behov av att behandla genetiska uppgifter. Regeringen delar därför utredningens bedömning att Säkerhetspolisen inte bör ges rätt att behandla genetiska uppgifter.

Att biometriska uppgifter behandlas särskilt är en lagteknisk fråga och innebär inte att de ska betraktas på något annat sätt än övriga kategorier av känsliga personuppgifter.

Behandling för diarieföring eller liknande

Enligt 2 kap. 10 § andra stycket och 6 kap. 4 § 4 polisdatalagen får Säkerhetspolisen behandla känsliga personuppgifter om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till myndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Som framgår av avsnitt 8.3.2 måste Säkerhetspolisen alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande anmälningar, ansökningar och andra liknande handlingar. Det bör gälla även i de fall där sådana handlingar innehåller känsliga personuppgifter, eftersom det ligger utanför Säkerhetspolisens kontroll om sådana uppgifter finns i handlingarna. Det bör därför framgå av den nya lagen att sådan behandling är tillåten. Bestämmelsen bör formuleras på motsvarande sätt som 2 kap. 13 § brottsdatalagen.

9.2.2 Ett sökförbud med undantag

Regeringens förslag: Det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Sökförbudet ska inte hindra att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning. Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för något av de syften som Säkerhetspolisen får behandla personuppgifter för.

Regeringens bedömning: Någon förändring av den sekretessreglering som är tillämplig i Säkerhetspolisens verksamhet behövs inte när det gäller uppgifter i sammanställningar av känsliga personuppgifter.

Utredningens förslag överensstämmer delvis med regeringens förslag och bedömning**.** Utredningen föreslår att det införs en regel om absolut sekretess till skydd för enskilda i offentlighets- och sekretesslagen (2009:400). Den absoluta sekretessen föreslås gälla hos Säkerhetspolisen för uppgift i en sammanställning av känsliga personuppgifter. Enligt förslaget ska sekretessen gälla i högst 70 år.

Remissinstanserna: *Säkerhetspolisen* förordar att bestämmelsen om sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter utformas på motsvarande sätt som i 6 kap. 11 § första stycket polisdatalagen. *Journalistförbundet* anser att undantaget i den föreslagna 2 kap. 12 § tredje stycket om att sökning på känsliga personuppgifter får göras om sökningen är absolut nödvändig för något av de syften som anges i 1 §, är för brett. Journalistförbundet avstyrker vidare förslaget om absolut sekretess och föreslår i stället att bestämmelsen förses med ett omvänt skaderekvisit. Även *Tidningsutgivarna* avstyrker förslaget om absolut sekretess och förordar att bestämmelsen utformas med ett rakt skaderekvisit.

Skälen för utredningens förslag och bedömning

Ny utformning av sökförbudet

Enligt 6 kap. 11 § polisdatalagen får Säkerhetspolisen använda känsliga personuppgifter som sökbegrepp vid sökning i personuppgifter som har gjorts gemensamt tillgängliga endast om det är absolut nödvändigt för de ändamål som myndigheten får behandla personuppgifter för. Brottsrubriceringar och uppgifter som beskriver en persons utseende får dock användas som sökbegrepp utan några begränsningar. Några begränsningar gäller inte heller vid sökning i personuppgifter som endast ett fåtal har tillgång till.

I 2 kap. 14 § brottsdatalagen finns ett generellt sökförbud som förbjuder sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Regeringen föreslog att det i övriga registerförfattningar skulle föreskrivas undantag från sökförbudet som är anpassade till de behov som respektive myndighet har (prop. 2017/18:232 s. 155–157 och t.ex. prop. 2017/18:269 s. 154–157). Frågan är om samma systematik bör väljas även för Säkerhetspolisen.

Vid polisdatalagens tillkomst ansåg regeringen att verksamhetsskäl talade för att Säkerhetspolisen inte borde förbjudas att använda känsliga personuppgifter som sökbegrepp, eftersom uppgifter av det slaget kan ha stor betydelse i myndighetens verksamhet. Regeringen framhöll samtidigt att verksamhetsintresset måste vägas mot intresset av att skydda de personer vilkas uppgifter behandlas mot intrång i den personliga integriteten. Vidare framhölls att utformningen av bestämmelsen om sökning gör att känsliga personuppgifter inte rutinmässigt kan användas som sökbegrepp utan först sedan det vid en prövning av behovet i det enskilda fallet konstaterats att det finns ett påtagligt behov (prop. 2009/10:85 s. 266).

Säkerhetspolisen har alltjämt behov av att kunna använda känsliga personuppgifter vid sökning. I arbetet med att förebygga och upptäcka terroristbrott kan t.ex. uppgifter om en persons politiska åsikter eller reli-

giösa övertygelse vara viktiga. Vid brott mot Sveriges säkerhet kan uppgifter av det slaget bidra till att fastställa motivet för gärningen. Säkerhetspolisen bör därför ges i huvudsak samma möjligheter som i dag att använda känsliga personuppgifter vid sökning.

Det skulle kunna hävdas att ett generellt sökförbud skulle bli innehållslöst då det skulle behöva förses med så många undantag. Regeringen anser dock att en reglering som bygger på ett generellt förbud med undantag som är anpassade för verksamheten ger en tydligare signal om att känsliga personuppgifter ska användas restriktivt. Det finns också fördelar med att regleringen för alla brottsbekämpande myndigheter överensstämmer i den delen. Regeringen anser därför, till skillnad mot *Säkerhetspolisen*, att regleringen i den nya lagen bör bygga på ett generellt förbud som utgår från syftet med sökningen liksom i brottsdatalagen. Förbudet bör på samma sätt som för övriga brottsbekämpande myndigheter gälla vid sökning i alla slags uppgifter, dvs. även i uppgifter som bara behandlas av ett fåtal. Från förbudet bör det göras undantag som tillgodoser Säkerhetspolisens behov av att kunna använda känsliga personuppgifter.

Genom att sökförbudet utgår från syftet med sökningen är sökning som inte görs i syfte att få fram ett personurval grundat på känsliga personuppgifter tillåten, även om känsliga personuppgifter används vid sökningen (jfr prop. 2017/18:232 s. 156.). Även tillåtna sökningar kan således resultera i ett personurval grundat på känsliga personuppgifter. I vilken utsträckning det är tillåtet att behandla personuppgifterna i en sådan sammanställning får prövas mot huvudregeln om behandling av känsliga personuppgifter.

Vilka undantag bör göras från sökförbudet?

Enligt 6 kap. 11 § andra stycket polisdatalagen är det tillåtet att använda brottsrubriceringar och uppgifter som beskriver en persons utseende som sökbegrepp. Säkerhetspolisen har också i fortsättningen behov av att kunna använda sådana uppgifter vid sökning, även om det leder till att man får fram ett personurval grundat på känsliga personuppgifter. I likhet med Polismyndigheten behöver Säkerhetspolisen också kunna söka på tillvägagångssätt vid brott, även om det skulle avslöja känsliga personuppgifter som t.ex. politiska åsikter (jfr prop. 2017/18:269 s. 154 f.). Det bör därför göras undantag från sökförbudet för sådana sökningar.

Regeringen föreslog att övriga brottsbekämpande myndigheter tillåts göra sökningar i syfte att få fram personurval grundade på vissa känsliga personuppgifter, under förutsättning att sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga (prop. 2017/18: 269 s. 155–157). För att Säkerhetspolisens sökmöjligheter ska vara desamma som i dag bör myndigheten även fortsättningsvis tillåtas att göra sökningar i syfte att få fram personurval grundade på i princip alla typer av känsliga personuppgifter. Även om det i dag inte finns någon begränsning när det gäller vilka uppgifter som får användas som sökbegrepp bör det emellertid inte vara tillåtet att ta fram personurval grundat på uppgifter som kan avslöja ras, eftersom det inte finns någon vetenskaplig grund för att dela in människor i skilda raser (jfr prop. 2017/18:232 s. 154). Säkerhetspolisen har enligt uppgift inte heller något behov av att göra

sökningar på medlemskap i fackförening. Det bör därför inte vara tillåtet att ta fram personurval grundade på sådana uppgifter.

Teknik för ansiktsigenkänning används i dag bl.a. för att underlätta identifiering när endast en del av ett ansikte är synligt på en bild eller en film eller om bildkvaliteten är dålig. Behandlingen i ett ansiktsigenkänningsprogram kan i sådana fall resultera i en träfflista med flera möjliga kandidater. Det skulle kunna hävdas att resultatet blir ett personurval grundat på biometriska uppgifter. Det är dock i dessa fall inte fråga om sökning i syfte att få fram ett visst personurval, utan om normal behandling av biometriska uppgifter. Sådan behandling föreslås vara tillåten om den är absolut nödvändig för ändamålet med behandlingen. Det finns därför enligt regeringens mening inte något behov av att göra undantag från sökförbudet för att sådan behandling ska vara tillåten.

Säkerhetspolisen får i dag använda känsliga personuppgifter som sökbegrepp vid sökning i alla slags uppgifter, dvs. oavsett om de har gjorts gemensamt tillgängliga eller inte. Eftersom Säkerhetspolisen även i fortsättningen bör tillåtas att göra sökningar i alla slags personuppgifter, går det inte att utforma undantaget på samma sätt som i övriga registerförfattningar. För att sökmöjligheterna inte ska bli alltför vida bör det på samma sätt som i dag krävas att det är absolut nödvändigt att göra sökningen. Kravet innebär att utrymmet för att göra sådana sökningar är begränsat och att rutinmässiga sökningar på känsliga personuppgifter inte är tillåtna.

Den nuvarande begränsningen i polisdatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter får användas vid sökning i uppgifter som enbart ett fåtal har tillgång till. Enligt 2 kap. 10 § polisdatalagen, som genom hänvisning i 6 kap. 4 § 4 gäller för Säkerhetspolisen, får känsliga personuppgifter dock bara behandlas om det är absolut nödvändigt för syftet med behandlingen och uppgifter om personen behandlas på annan grund. Den begränsningen gäller även vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga. Att det föreslagna sökförbudet och undantagen från det kommer att gälla vid sökningar i alla slags personuppgifter bör därför inte innebära några större förändringar när det gäller Säkerhetspolisens möjligheter att använda känsliga personuppgifter vid sökning. Vad *Journalistförbundet* anför i denna del föranleder därför ingen annan bedömning.

Ingen förändring av sekretessregleringen för sammanställningar av känsliga personuppgifter

Regeringen föreslår att det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Enligt utredningen bör det införas en sekretessregel som knyts till regeln om sökförbud i den nya lagen. Utredningens skäl för att införa en sådan sekretessregel är att allmänheten inte med stöd av offentlighetsprincipen ska kunna få ut uppgifter i sammanställningar som utgör resultatet av sådana sökningar som sökförbudet är avsett att förhindra. Enligt utredningens förslag ska sekretessen vara absolut så att Säkerhetspolisen inte

ska behöva göra en otillåten sökning för att kunna bedöma sekretessfrågan om uppgifter begärs ut (jfr prop. 2011/12:157 s. 17).

I likhet med utredningen anser regeringen att det är av stor vikt att enskildas integritet skyddas. Det rör sig om personuppgifter som omgärdas av starka dataskyddsregler. Redan i dag finns sekretessreglering som skulle aktualiseras om allmänheten begär ut känsliga personuppgifter som sammanställts av Säkerhetspolisen genom sökning. Som exempel kan nämnas att det i 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen finns sekretessregler till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. I 35 kap. 1 § samma lag finns en regel om sekretess till skydd för enskildas intressen i förundersökning och annan brottsbekämpande verksamhet. Enligt 21 kap. 7 § offentlighets- och sekretesslagen gäller vidare sekretess för personuppgifter om det kan antas att uppgifterna efter ett utlämnande kommer att behandlas i strid med regleringen om hur personuppgifter får behandlas. Den befintliga sekretessregleringen ger enligt regeringens bedömning ett väl avvägt skydd för både enskilda och allmänna intressen i nu aktuellt avseende. Till skillnad från utredningen ansåg regeringen därför att sökförbudet i brottsdatalagen inte behövde kompletteras av en regel om absolut sekretess för uppgifter i sammanställningar av känsliga personuppgifter (prop. 2017/18:232 s. 416 f.) Regeringen gör samma bedömning vad gäller sekretess för sammanställningar av känsliga personuppgifter hos Säkerhetspolisen. Någon ändring av den sekretessreglering som är tillämplig i Säkerhetspolisens verksamhet när det gäller uppgifter i sådana sammanställningar behövs därför inte.

9.3 Åtgärder för att säkerställa personuppgifternas kvalitet

Regeringens förslag: Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga rättas utan onödigt dröjsmål. Detsamma gäller för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas på ett otillåtet sätt utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

I stället för att personuppgifterna raderas, ska behandlingen av uppgifterna begränsas utan onödigt dröjsmål om uppgifterna behöver finnas kvar av bevisskäl.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering och bestämmelserna i brottsdatalagen

Enligt 9 § första stycket h personuppgiftslagen ska alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 3 och 6 kap. 4 § 1 polisdatalagen.

Bestämmelserna i brottsdatalagen, som reglerar den personuppgiftsansvariges skyldighet att på eget initiativ rätta, radera eller begränsa behandlingen av personuppgifter, är mer detaljerade och anger på ett tydligare sätt när de olika åtgärderna ska vidtas. Enligt 2 kap. 15 § första stycket brottsdatalagen ska alla rimliga åtgärder vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt. När personuppgifter lämnas ut till en behörig myndighet, ska mottagaren så långt det är möjligt ges information som gör det möjligt att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga. Enligt 2 kap. 16 § ska alla rimliga åtgärder vidtas för att personuppgifter som behandlas på ett otillåtet sätt utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse. I stället för att radera personuppgifterna ska den personuppgiftsansvarige utan onödigt dröjsmål begränsa behandlingen av dem, om de behöver finnas kvar av bevisskäl. Regleringen i brottsdatalagen utgår alltså från att felaktiga personuppgifter ska rättas och att personuppgifter som behandlas på ett otillåtet sätt ska raderas.

Regleringen ska i huvudsak motsvara regleringen i brottsdatalagen

När det gäller skyldigheten att på eget initiativ rätta, radera eller begränsa behandlingen av felaktiga eller ofullständiga personuppgifter eller personuppgifter som behandlats på ett otillåtet sätt anser regeringen, i likhet med utredningen, att i princip samma krav bör ställas på Säkerhetspolisen som på övriga brottsbekämpande myndigheter. Det gäller även ansvaret att se till att felaktiga eller ofullständiga uppgifter inte lämnas ut eller görs tillgängliga. Det bör därför i den nya lagen tas in bestämmelser med samma innebörd som 2 kap. 15 och 16 §§ brottsdatalagen.

Kravet på information i samband med utlämnande eller tillgängliggörande av personuppgifter som regleras i 2 kap. 15 § andra stycket brottsdatalagen har sin grund i dataskyddsdirektivet. Något sådant krav ställs inte på Säkerhetspolisen i dag. Det ligger i sakens natur att Säkerhetspolisen inte i samma utsträckning som andra brottsbekämpande myndigheter kan avslöja vilken information som ligger till grund för t.ex. en misstanke om någons delaktighet i brottslig verksamhet. Någon motsvarande bestämmelse bör därför inte tas in i den nya lagen.

Om det upptäcks att felaktiga personuppgifter eller personuppgifter som behandlas på ett otillåtet sätt har lämnats ut är det naturligt att den som har fått uppgifterna underrättas, så att uppgifterna kan rättas eller raderas eller

behandlingen av dem begränsas (prop. 2017/18:232 s. 162). Underrättelseskyldigheten kan regleras i förordning.

9.4 Personuppgifter från transportföretag

Regeringens förslag: Bestämmelserna om behandling av personuppgifter som tillhandahålls av transportföretag enligt polislagen ska tas in i den nya lagen. Sådana personuppgifter ska endast i enskilda fall få behandlas för nya ändamål.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag. Utredningen föreslår dock att personuppgifter från transportföretag endast ska få behandlas för vissa syften.

Remissinstanserna: Endast *Säkerhetspolisen* yttrar sig i denna del och avstyrker bestämmelsen om att uppgifter från transportföretag endast får behandlas för vissa syften eftersom det innebär en begränsning i förhållande till vad som gäller i dag.

Skäl för regeringens förslag

Nuvarande reglering

Enligt 25 § polislagen (1984:387) är transportföretag skyldiga att på begäran skyndsamt lämna vissa personuppgifter till Polismyndigheten och Säkerhetspolisen. Det rör sig bl.a. om uppgifter om resenärers namn, medresenärers namn och transportmedel.

Personuppgifterna får tillhandahållas genom terminalåtkomst till transportföretagens bokningssystem där polisen får läsa uppgifterna. Terminalåtkomst tillåts enligt 26 § polislagen bara i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. Uppgifterna får även lämnas på annat sätt om transportföretaget anser att det är bättre. Uppgifterna lämnas ofta elektroniskt, men det förekommer även att de tillhandahålls på papper.

Personuppgiftsbehandlingen bör regleras i den nya lagen

I polislagen reglerades tidigare inte bara transportföretagens uppgiftsskyldighet utan även på vilket sätt och hur länge polisen fick behandla personuppgifterna. Regeringen föreslog i propositionen Brottsdatalag – kompletterande lagstiftning att bestämmelserna om hur personuppgifter från transportföretag får behandlas skulle föras över till polisens brottsdatalag. Bakgrunden till det var att det inte fanns någon reglering av behandling av personuppgifter från transportföretag i polisdatalagen. Inom brottsdatalagens tillämpningsområde är dock utgångspunkten att myndigheternas personuppgiftsbehandling i så stor utsträckning som möjligt ska regleras i respektive myndighets registerförfattning. En annan ordning, med enstaka bestämmelser om personuppgiftsbehandling i andra lagar, skulle innebära att regleringen blir mer svåröverskådlig för enskilda (prop. 2017/18:232 s. 158). Dessa skäl har även giltighet för Säkerhetspolisen. Regleringen av hur Säkerhetspolisen får behandla personuppgifter som transportföretag på begäran tillhandahåller

myndigheten enligt polislagen bör därför tas in i den nya lagen. Transportföretagens skyldigheter bör dock, på samma sätt som för Polismyndighetens del, fortfarande regleras i polislagen.

Hur får uppgifterna behandlas?

Utredningen föreslår att Säkerhetspolisen på samma sätt som Polismyndigheten ska få behandla personuppgifter från transportföretag endast för vissa syften. *Säkerhetspolisen* har invänt att det innebär en begränsning i förhållande till vad som gäller i dag och att behovet av uppgifter från transportföretag kan förekomma i hela myndighetens verksamhet. Enligt 25 § andra stycket polislagen är Polismyndighetens möjligheter att begära uppgifter från transportföretag begränsade till uppgifter som kan antas ha betydelse för den brottsbekämpande verksamheten. Av förarbetena till den ändring av bestämmelsen som gjordes i samband med polisomorganisationen framgår att Säkerhetspolisen inte behöver anges i bestämmelsen eftersom myndigheten enbart bedriver brottsbekämpande verksamhet (En ny organisation för polisen, del 1, prop. 2013/14:110, s. 581). Som framgår av avsnitt 7.3 anses all Säkerhetspolisens verksamhet vara brottsbekämpande och lagförande. Det är inte någon förändring i sak jämfört med tidigare ställningstaganden utan hänger samman med att uttrycket brottsbekämpande verksamhet har fått en snävare innebörd genom brottsdatalagens införande. Den begränsning som utredningen föreslår finns alltså inte i dagens reglering. Mot den bakgrunden och eftersom behovet av uppgifter från transportföretag kan förekomma i Säkerhetspolisens hela verksamhet anser regeringen att myndighetens möjligheter att begära uppgifter från transportföretag inte bör begränsas till om uppgifterna behövs för vissa syften.

Transportföretagen får, som framgår av 26 § polislagen, tillhandahålla Polismyndigheten och Säkerhetspolisen passageraruppgifter genom att göra dem läsbara via terminalåtkomst. Tidigare föreskrevs också att uppgifter som hålls tillgängliga på det sättet inte fick ändras eller på annat sätt bearbetas eller lagras av myndigheterna. Bestämmelsen kunde uppfattas på det sättet att myndigheterna inte fick hantera personuppgifterna på annat sätt än att läsa dem på en terminal. Det kunde dock inte ha varit avsikten att regleringen skulle tolkas så snävt, eftersom tillgången till sådana uppgifter skulle vara meningslös om uppgifter av betydelse för brottsbekämpningen inte skulle få tillföras den brottsbekämpande verksamheten. I förarbetena till polisens brottsdatalag ansåg regeringen därför att det borde förtydligas att bestämmelsen endast hindrar ändring eller bearbetning av uppgifterna i transportbolagens itsystem (prop. 2017/18:269 s. 158 f.). Ett motsvarande förtydligande bör tas in i den nya lagen.

Uppgifterna från transportföretagen är till allra största delen information om personer som inte är intressanta ur ett brottsbekämpningsperspektiv. Utgångspunkten är därför att uppgifterna ska ges så liten spridning som möjligt. Säkerhetspolisen bör liksom Tullverket och Polismyndigheten få göra uppgifter från transportföretag gemensamt tillgängliga vid behov (jfr prop. 2017/18:269 s. 161). Det kan vara uppgifter om någon eller några personer eller transporter som är av betydelse i underrättelseverksamheten eller i en brottsutredning som görs gemensamt tillgängliga.

Säkerhetspolisen får göra personuppgifter gemensamt tillgängliga om det behövs för några av de uppgifter för vilka Säkerhetspolisen får behandla personuppgifter (avsnitt 8.3.1). Någon särskild reglering behövs därför inte.

Tidigare angavs i 26 § tredje stycket polislagen att uppgifter om enskilda personer som ett transportföretag lämnat på annat sätt än genom terminalåtkomst omedelbart skulle förstöras om de visade sig sakna betydelse för utredning av eller lagföring för brott. Bestämmelsen upphävdes i samband med införandet av polisens brottsdatalag, eftersom uppgifterna får tillräckligt skydd genom bestämmelsen i 2 kap. 17 § första stycket brottsdatalagen om att personuppgifter inte får behandlas under längre tid än som är nödvändigt med hänsyn till ändamålet med behandlingen (prop. 2017/18:269 s. 161 f.). En motsvarande bestämmelse föreslås tas in i den nya lagen (avsnitt 12.2.1), och någon särskild reglering om hur länge personuppgifter från transportföretag får behandlas behövs därför inte.

Behandling för nya ändamål

I dag finns det ingen bestämmelse om vidarebehandling av personuppgifter som transportföretag tillhandahåller. Regeringen konstaterar i förarbetena till polisens brottsdatalag att riksdagen nyligen har ställt sig bakom att Tullverket ska få behandla personuppgifter av nu aktuellt slag för nya ändamål endast om det behövs i enskilda fall. Mot den bakgrunden ansåg regeringen att polisens rätt att behandla personuppgifter som tillhandahålls av transportföretag för nya ändamål bör begränsas på motsvarande sätt (prop. 2017/18:269 s. 160 f.). Det bör gälla även för Säkerhetspolisen.

Det bör inte regleras vilka sökbegrepp som får användas

I dag gäller inga begränsningar i polisens möjligheter att söka i uppgifter från transportföretag. Utredningen föreslog att sådana begränsningar skulle införas för Polismyndigheten men inte för Säkerhetspolisen. I förarbetena till polisens brottsdatalag konstaterade regeringen att den föreslagna sökbegränsningen kunde riskera att försämra Polismyndighetens möjligheter att bekämpa den organiserade gränsöverskridande brottsligheten och någon sökbegränsning infördes därför inte (prop. 2017/18:269 s. 159 f.). Säkerhetspolisens användning av direkta personuppgifter vid sökning i uppgifter från transportföretag bör därför inte heller begränsas.

Lagen om flygpassageraruppgifter i brottsbekämpningen har företräde

Lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen innehåller bl.a. bestämmelser om personuppgiftsbehandling i enlighet med kraven i det s.k. PNR-direktivet. Där regleras skyldigheten för flygbolag att överföra passageraruppgiftssamlingar till särskilda enheter för passagerarinformation i medlemsstaterna, för vilka ändamål personuppgifterna får behandlas, hur länge de får lagras och under vilka förutsättningar de får lämnas ut. Lagen om flygpassageraruppgifter i brottsbekämpningen kommer att ha företräde framför bestämmelserna i den nya lagen (avsnitt 7.6).

10 Gemensamt tillgängliga uppgifter

10.1 Samma reglering av vad som får göras gemensamt tillgängligt

Regeringens förslag: Särskilda bestämmelser ska gälla för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

Personuppgifter ska få göras gemensamt tillgängliga om det behövs för någon av de uppgifter som Säkerhetspolisen får behandla personuppgifter för.

Bestämmelserna om gemensamt tillgängliga uppgifter ska inte gälla när personuppgifter behandlas med stöd av bestämmelsen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 6 kap. polisdatalagen (2010:361) finns särskilda bestämmelser som gäller vid behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Med gemensamt tillgängliga uppgifter avses uppgifter som inte enbart ett fåtal har tillgång till. För behandling av sådana uppgifter ställs det t.ex. krav på särskilda upplysningar och vidare begränsas möjligheten till sökning. Sådana bestämmelser bör finnas även i den nya lagen. För att få en enhetlig systematik bör regleringen om gemensamt tillgängliga uppgifter finnas i ett särskilt kapitel.

Av 6 kap. 8 § polisdatalagen framgår att personuppgifter får göras gemensamt tillgängliga i Säkerhetspolisens verksamhet om det behövs för något av de ändamål för vilka personuppgifter får behandlas. I förarbetena till polisdatalagen konstaterar regeringen att de intressen som Säkerhetspolisen har till uppgift att skydda motiverar att myndigheten ges större handlingsfrihet i fråga om vilka uppgifter som får göras gemensamt tillgängliga. Skälet till det är bl.a. att Säkerhetspolisens verksamhet är inriktad mot brottslighet som till sin natur är svår att upptäcka och att tyngdpunkten i dess brottsbekämpande arbete ligger på underrättelsearbete och renodlat förebyggande arbete. Det konstateras vidare att det är svårt att förutse och i lag uttrycka de olika kategorier av personuppgifter som bör få göras gemensamt tillgängliga hos Säkerhetspolisen och att myndighetens verksamhet till sin natur är sådan att informationen sprids i mindre utsträckning än inom polisen i övrigt (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 264).

Enligt regeringens mening är de skäl som anges i förarbetena till polisdatalagen fortfarande aktuella. Regleringen av när personuppgifter får göras gemensamt tillgängliga bör därför i princip tas in oförändrad i den nya lagen. Den bör dock knytas till bestämmelsen om rättslig grund och de uppgifter för vilka Säkerhetspolisen får behandla personuppgifter, i stället för till ändamålen med behandlingen.

I 6 kap. 8 § andra stycket polisdatalagen föreskrivs att bestämmelserna om gemensamt tillgängliga uppgifter inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter. En motsvarande bestämmelse bör tas in i den nya lagen.

10.2 Särskilda upplysningar

Regeringens förslag: Om det ändamål som gemensamt tillgängliga personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet som omfattas av lagens tillämpningsområde, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha direkt samband med brottslig verksamhet ska som regel förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av omständigheterna är onödigt.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Datainspektionen* avstyrker utredningens förslag att kravet på särskilda upplysningar enbart ska gälla om personuppgifterna har gjorts gemensamt tillgängliga. Behoven av undantag kan regleras på motsvarande sätt som i 2 kap. 9 § brottsdatalagen genom att det anges att kravet gäller ”så långt det är möjligt”. Inspektionen anser vidare att det i stället för en upplysning om att någon inte är misstänkt bör föreskrivas att olika kategorier av registrerade, t.ex. misstänkta, brottsoffer och vittnen, ska särskiljas. Datainspektionen anser också att kravet på särskilda upplysningar ska gälla när uppgifter såväl ”direkt som indirekt kan hänföras till en person som inte är misstänkt”. *Säkerhets- och integritetsskyddsnämnden* föreslår att bestämmelsen om särskilda upplysningar om misstanke ska formuleras på ett annat sätt för att det ska bli tydligare när kravet gäller.

Skälen för regeringens förslag

Särskild upplysning om ändamålet med behandlingen

Enligt 6 kap. 9 § polisdatalagen ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifter som har gjorts gemensamt tillgängliga behandlas. Både av hänsyn till verksamheten och till den personliga integriteten är det viktigt att det framgår för vilket ändamål en personuppgift behandlas. Från integritetssynpunkt har det betydelse bl.a. för möjligheterna att genom tekniska förfaranden eller administrativa bestämmelser kunna styra åtkomsten till vissa uppgifter. Att ändamålet med behandlingen framgår kan vidare vara en förutsättning för att en tillsynsmyndighet ska kunna kontrollera om viss behandling är berättigad och utförs i enlighet med lagens bestämmelser.

Information om ändamålet med behandlingen behövs också för att de tjänstemän som får tillgång till personuppgifter ska kunna värdera uppgifterna korrekt och använda sig av dem på ett effektivt och lagenligt sätt. Informationen behövs bl.a. för att kunna ta ställning till om uppgiften får och bör behandlas för ett nytt ändamål. En bestämmelse som föreskriver att det ska framgå för vilket ändamål personuppgifter behandlas bör därför tas in i den nya lagen. På samma sätt som i dag bör dock särskilda upplysningar krävas endast om ändamålet inte framgår av sammanhanget eller på något annat sätt. Bestämmelsen bör formuleras på samma sätt som 2 kap. 3 § andra stycket brottsdatalagen.

Upplysning om att den registrerade inte är misstänkt

Om uppgifter direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det enligt 6 kap. 10 § första stycket polisdatalagen genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Det är av stor betydelse för skyddet av den personliga integriteten vid brottsbekämpning att personuppgifter behandlas på ett sådant sätt att det framgår om en person är misstänkt eller inte. Ofta framgår det av omständigheterna eller sammanhanget i vilket personuppgifterna behandlas att en uppgift avser en person som inte är misstänkt. Det är främst i det inledande skedet av en förundersökning och i underrättelseverksamhet som det kan vara otydligt vilken roll en person har och det är framför allt när uppgifter behandlas utanför sitt ursprungliga sammanhang som särskilda upplysningar kan behövas. Det bör därför tas in en bestämmelse i den nya lagen om att det ska framgå om personuppgifter direkt hänför sig till en person som inte är misstänkt för att ha utövat brottslig verksamhet. Det bör tydliggöras att upplysningen ska avse brott eller brottslig verksamhet som Säkerhetspolisen har till uppgift att bekämpa. Bestämmelsen bör formuleras på det sätt *Säkerhets- och integritetsskyddsnämnden* föreslår för att det ska bli tydligt när kravet på särskild upplysning gäller.

I 2 kap. 9 § brottsdatalagen (2018:1177) föreskrivs att så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade, som personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott, särskiljas. Om det inte framgår av sammanhanget eller på något annat sätt vilken kategori personen tillhör, ska det tydliggöras genom en särskild upplysning. *Datainspektionen* anser att den modellen bör användas även i den nya lagen i stället för att det bara ska framgå att någon inte är misstänkt. Kravet på att olika kategorier av registrerade ska särskiljas har sin grund i dataskyddsdirektivet. Med hänsyn till att Säkerhetspolisen ofta behandlar personuppgifter i ett tidigt skede i sin underrättelseverksamhet, då det normalt inte går att urskilja lika tydliga kopplingar till konkreta brott eller brottslig verksamhet som inom Polismyndigheten, och det då är svårt att veta vilken roll olika personer har, är det inte rimligt att fler kategorier av personer ska särskiljas. Det bör därför inte krävas mer än att det framgår om en person inte är misstänkt.

Datainspektionen har vidare ansett att kravet på särskilda upplysningar ska gälla när uppgifter såväl ”direkt som indirekt kan hänföras till en person som inte är misstänkt”. Uttrycket ”uppgifter som direkt kan hänföras

till en person” finns redan i dag i 6 kap. 10 § första stycket polisdatalagen. Motsvarande skrivning finns också i 3 kap. 4 § polisens brottsdatalag. Utredningen föreslår inte någon ändring. Regeringen anser inte heller att det finns skäl att ändra lagtexten i denna del utifrån vad *Datainspektionen* anfört.

Upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak

I 6 kap. 10 § andra stycket polisdatalagen ställs det krav på att uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon upplysning krävs dock inte om det på grund av särskilda omständigheter är onödigt eller om uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede.

På samma sätt som det är viktigt att det framgår om en uppgift rör en icke misstänkt person, är det viktigt att det framgår hur tillförlitlig en underrättelseuppgift bedöms vara. Syftet med en sådan bestämmelse är dels att stärka skyddet för den enskildes integritet, dels att förhindra att uppgifter, vilkas tillförlitlighet och trovärdighet är begränsad, läggs till grund för bedömningar och åtgärder som inte är sakligt motiverade (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 265). En motsvarande bestämmelse bör därför tas in i den nya lagen.

Kravet på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak bör endast avse uppgifter om den som kan antas utöva eller komma att utöva den brottsliga verksamheten. Eftersom det krav som gäller för anknytningen till den brottsliga verksamheten således är mycket lågt ställt träffar regleringen en relativt vid personkrets. Så snart det finns något som stöder ett antagande om att en person har direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga bör således uppgifterna om personen förses med särskild upplysning. Det är vidare endast sådana uppgifter som belyser på vilket sätt personen är knuten till brottsligheten som bör förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det kan, förutom anknytningen till den brottsliga verksamheten, t.ex. röra sig om uppgifter om brottslighetens art och omfattning. Uppgifter av det slaget kan behöva förses med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas (jfr Brottsdatalag – kompletterande lagstiftning, prop. 2017/18:269, s. 111).

På samma sätt som i dag bör det göras undantag från kravet på särskild upplysning om det inte finns något behov av en sådan därför att det framgår av sammanhanget vem som är uppgiftslämnare och hur trovärdig uppgiften är eller det av annat skäl är onödigt med en sådan upplysning. Den nuvarande formuleringen av bestämmelsen innebär att det krävs särskild upplysning om det inte på grund av särskilda omständigheter är onödigt. Det har framkommit att det anses vara oklart vilka särskilda omständigheter som kan föranleda avsteg från huvudregeln och att det har lett till en omotiverat restriktiv tillämpning. Regeringen har därför i

propositionen Brottsdatalag – kompletterande lagstiftning föreslagit att regleringen ska ändras så att det ställs krav på särskilda upplysningar om det inte på grund av omständigheterna är onödigt. Med en sådan formulering undviker man den osäkerhet som kan finnas om vilken typ av omständigheter som kan göra behovet av särskilda upplysningar överflödigt. Om de samlade omständigheterna gör att trovärdigheten och riktigheten kan bedömas bör det vara tillräckligt (prop. 2017/18:269 s. 111 f.). Samma formulering bör användas i den nya lagen. Regeringen återkommer i avsnitt 10.3 till undantaget för ostrukturerad underrättelseinformation.

Särskilda upplysningar bara om uppgifterna är gemensamt tillgängliga

Kraven på särskilda upplysningar i 6 kap. 9 och 10 §§ gäller enligt nuvarande reglering endast uppgifter som har gjorts gemensamt tillgängliga. I förarbetena till polisdatalagen diskuteras ingående skälen för att ha sådana bestämmelser och när särskilda upplysningar inte behövs (prop. 2009/10:85 s. 145 f.). När ett fåtal personer behandlar uppgifterna och är införstådda med varför det görs finns det inget behov av särskilda upplysningar. I dessa fall tillgodoses integritetsskyddet som de särskilda upplysningarna syftar till att skapa på annat sätt. Behovet av särskilda upplysningar gör sig således framför allt gällande om personuppgifter behandlas utanför sitt ursprungliga sammanhang. Regeringen anser därför, till skillnad från *Datainspektionen*, att kravet på särskilda upplysningar på samma sätt som i dag enbart ska gälla vid behandling av personuppgifter som har gjorts gemensamt tillgängliga.

10.3 Undantag från kravet på särskild upplysning

10.3.1 Behandling av personuppgifter i ostrukturerad information

Informationsmängden ökar ständigt

Säkerhetspolisen tar varje dag emot stora mängder information i olika former och från olika källor. Informationsflödet påverkas av vad som händer i omvärlden och är av naturliga skäl som mest intensivt i samband med särskilda händelser. Som exempel kan nämnas när media publicerade information om en person som vistades i Sverige och som befarades inom kort skulle utföra ett terroristattentat. Det resulterade i en oerhört stor mängd tips från allmänheten. Samtidigt var informationsutbytet intensivt både nationellt och internationellt. Motsvarande kraftiga informationsflöde uppkom vid attentatet på Drottninggatan i Stockholm i april 2017. Även händelser utomlands kan periodvis generera stora mängder information. Säkerhetspolisen kan också förväntas få ta emot allt större informationsmängder generellt.

Bearbetning och analys av underrättelseinformation

Alla handlingar som kommer in till eller upprättas vid Säkerhetspolisen diarieförs i myndighetens dokument- och ärendehanteringssystem. Den första bedömningen av uppgifterna görs så snart som möjligt av ansvarig

handläggare i det systemet. Om uppgifterna behöver behandlas i Säkerhetspolisens underrättelseverksamhet förs de därefter som regel över till it-systemet för bearbetning och analys. Det systemet innehåller två delar. Den ena delen är en uppgiftssamling med uppgifter för bearbetning och analys och den andra en uppgiftssamling med bedömd information.

När en handling har tillförts uppgiftssamlingen för bearbetning och analys bedöms den även av en särskild granskningsfunktion. Granskningen syftar bl.a. till att säkerställa att Säkerhetspolisen överhuvudtaget får behandla uppgifterna. Behovet av att behandla känsliga personuppgifter prövas särskilt. Känsliga personuppgifter som inte får behandlas tas bort genom maskning. Därefter bearbetas informationen genom att uppgifterna bryts ut och kopplas samman med annan information, tematiseras och tillförs särskilda upplysningar om det krävs.

När bearbetningen är klar kan uppgifterna föras över till uppgiftssamlingen med bedömd information eller tas bort. Det förekommer dock att uppgifterna ligger kvar i uppgiftssamlingen med uppgifter under bearbetning och analys även en tid efter det att bearbetningen är färdig. Det framgår dock att bearbetningen av uppgifterna är klar.

Särskilda bestämmelser för gemensamt tillgängliga uppgifter

När det gäller ostrukturerad information dvs. uppgifter som är under bearbetning och analys, kan det vara svårt för Säkerhetspolisen att uppfylla vissa av de krav som ställs på gemensamt tillgängliga uppgifter. Svårigheten gäller främst kravet i 6 kap. 10 § andra stycket polisdatalagen på upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak (avsnitt 10.2). Uppgifterna kan normalt inte förses med sådana upplysningar förrän de har bearbetats. Därför görs det i 6 kap. 10 § andra stycket undantag från kravet på sådan upplysning, om personuppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede. Enligt förarbetena ska det vara fråga om en kortare period (prop. 2009/10:85 s. 370 f.).

10.3.2 Det befintliga undantaget bör justeras

Regeringens förslag: Gemensamt tillgängliga personuppgifter ska inte behöva förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till, och
2. bearbetningen av uppgifterna inte har genomförts.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Endast *Säkerhets- och integritetsskyddsnämnden* yttrar sig i denna del och anför att det inte av betänkandet går att läsa ut när bearbetningen av uppgifterna kan anses genomförd. Som undantaget är formulerat finns det därför en risk att kravet på särskild upplysning inte kommer att uppfyllas i uppgiftssamlingar för bearbetning och analys.

Skälen för regeringens förslag

Bör undantaget justeras?

Som framgår av avsnitt 10.3.1 är det inte meningen att ostrukturerad underrättelseinformation ska behandlas i en uppgiftssamling för bearbetning och analys någon längre tid utan att den bearbetas. Utgångspunkten är att analysen av den ostrukturerade informationen ska genomföras så snabbt som möjligt. På grund av den omfattande mängd information som periodvis kan komma in till Säkerhetspolisen har myndigheten dock inte alltid möjlighet att strukturera de uppgifter som förs in i uppgiftssamlingen för bearbetning och analys så snabbt som förutsätts i 6 kap. 10 § andra stycket polisdatalagen. Konsekvensen blir att uppgifterna inte kan göras gemensamt tillgängliga, eftersom de inte helt uppfyller de krav som ställs på sådana uppgifter.

Säkerhetspolisen behöver emellertid kunna tillgängliggöra sådan ostrukturerad information till fler än det fåtal tjänstemän som arbetar med bearbetning och analys och i vissa fall under längre tid än under ett inledande skede. Det finns risk för att relevant information inte kommer den operativa verksamheten till del om den inte kan göras gemensamt tillgänglig. En konsekvens kan bli att viktig information om t.ex. nära förestående attentat inte upptäcks i tid. Om sådan information inte tillgängliggörs förrän den är färdigbearbetad kan det också leda till att Säkerhetspolisens förmåga att identifiera, bedöma och reducera hot och sårbarheter minskar. Tillgång till ostrukturerad information är enligt uppgift särskilt viktig för att kunna identifiera aktörer som agerar ensamma.

Säkerhetspolisen har till uppgift att skydda grundläggande samhällsfunktioner och att bekämpa terrorism. Vid en intresseavvägning mellan verksamhetens behov och enskildas integritet väger därför verksamhetsintresset tyngre än annars. Att tillåta att information tillgängliggörs i något större utsträckning än i dag trots att den inte hunnit struktureras och, där det krävs, förses med särskilda upplysningar får mot den bakgrunden accepteras. Det befintliga undantaget från kravet på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak bör därför justeras.

Utformningen av undantaget

I Säkerhetspolisens underrättelsearbete är utgångspunkten att uppgifter som inte har bedömts och tillförts en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak varken kan läggas till grund för beslut, bedömningar eller åtgärder. Personalen är således van vid att hantera svårbedömd information och det finns, enligt myndigheten, tydliga rutiner för hur ostrukturerad information ska behandlas. Risken för att sådan information leder till felbedömningar och åtgärder som inte är sakligt motiverade anses mot den bakgrunden vara liten.

De skäl som har förts fram för att tillåta att ostrukturerad information får tillgängliggöras i större utsträckning än i dag gör att undantaget bör omformuleras. Det är först när bearbetningen är genomförd som det är möjligt att påföra de särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak som krävs i vissa fall. Undantaget bör därför gälla fram till dess att bearbetningen av uppgifterna är genomförd. Viktig underrättelseinformation kan då vid behov göras

gemensamt tillgänglig på ett sätt som bättre svarar mot Säkerhetspolisens behov. *Säkerhets- och integritetsskyddsnämnden* anser att formuleringen inte gör det tydligt hur länge undantaget gäller, eftersom det inte framgår när bearbetningen är genomförd. Enligt uppgift från Säkerhetspolisen framgår det tydligt i systemet när bearbetningen är genomförd och kravet på särskilda upplysningar bedömt. Det framstår också som naturligt att det är så, eftersom verksamheten är beroende av att det klargörs när informationen är bedömd så att den kan läggas till grund för eventuella åtgärder och beslut. Regeringen anser därför att undantaget både är tillräckligt tydligt och på ett tillfredställande sätt tillgodoser Säkerhetspolisens behov av ett något generösare undantag från kravet på särskilda upplysningar. Utgångspunkten är dock fortfarande att Säkerhetspolisen ska genomföra bearbetningen och analysen av den ostrukturerade informationen så snart som möjligt.

Det är viktigt att understryka att hela uppgiftssamlingen för bearbetning och analys inte undantas från kravet på särskilda upplysningar. Undantaget omfattar endast sådana uppgifter i uppgiftssamlingen som inte har hunnit bearbetas. Så snart bearbetningen är genomförd och informationen strukturerad är undantaget inte längre tillämpligt. Personuppgifterna ska då förses med särskilda upplysningar om det behövs.

När ska behandlingen senast upphöra?

I avsnitt 12.2.3 föreslås att personuppgifter i en uppgiftssamling för bearbetning och analys som längst ska få behandlas tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Som framgår av avsnitt 12.2.1 får personuppgifter dock aldrig behandlas under längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Behandlingen ska således upphöra även om tidsfristen om tre år inte har löpt ut om uppgiften inte längre behövs för ändamålet med behandlingen. Det förutsätter dock att det går att bedöma om behandlingen är nödvändig för ändamålet. Huvudregeln ger således stöd för fortsatt behandling så länge uppgifterna behövs för något av de tillåtna ändamålen. Det finns därför stöd för fortsatt behandling om Säkerhetspolisen t.ex. bedömer att uppgifterna allmänt är värdefulla för att förebygga, förhindra och upptäcka brottslig verksamhet (prop. 2009/10:85 s. 327 och 367 f.).

När det gäller ostrukturerad underrättelseinformation ligger det i sakens natur att det är svårt att bedöma det fortsatta behovet av behandling. Bedömningen måste innan bearbetningen och analysen är klar göras på ett mer övergripande plan och i större utsträckning utgå från sannolikheten att uppgifterna kan komma att behövas i verksamheten än en reell bedömning av den enskilda uppgiften. Enligt regeringens mening kan det vid en sådan övergripande bedömning ofta finnas behov av fortsatt behandling av den ostrukturerade informationen för något av de ändamål som är tillåtna enligt lagen.

11 Informationsutbyte

11.1 Behovet av att kommunicera elektroniskt har ökat

11.1.1 Olika former av elektroniskt utlämnande

Direktåtkomst

Det finns inte någon legaldefinition av uttrycket direktåtkomst. Det som vanligtvis avses med direktåtkomst är att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Enligt Informationshanteringsutredningen bör direktåtkomst anses föreligga om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (Myndighetsdatalag, SOU 2015:39, s. 390 f.). Högsta förvaltningsdomstolen har använt samma definition av direktåtkomst (HFD 2015 ref. 61). I begreppet direktåtkomst ligger också att den som är personuppgiftsansvarig för registret eller databasen saknar kontroll över vilka uppgifter som den som har direktåtkomst vid ett visst tillfälle tar del av. Från integritetssynpunkt har det därför ansetts viktigt att frågor om tillgång till uppgifter genom direktåtkomst regleras särskilt i registerlagstiftningarna (Ökat informationsutbyte mellan arbetslöshetsförsäkringen, socialförsäkringen och studiestödet, prop. 2000/01:129, s. 74, Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, prop. 2001/02:144, s. 35 f. och Elektronisk informationsöverföring hos arbetslöshetskassorna och inom Arbetsmarknadsverket, prop. 2005/06:52, s. 8).

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

Utlämnande på medium för automatiserad behandling

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

Utlämnande av personuppgifter på medium för automatiserad behandling kan alltså göras på många olika sätt. Det kan vara fråga om att personuppgifter lämnas t.ex. via e-post eller usb-minne. Begreppet anses

omfatta överlämnande av elektroniskt lagrade uppgifter via alla slags medium för lagring och överföring (Överskottsinformation vid direktåtkomst, SOU 2012:90, s. 198).

Risker med elektroniskt utlämnande

Elektroniskt utlämnande av personuppgifter kan anses medföra risker från integritetssynpunkt. Sådant utlämnande innebär nämligen som regel att mottagaren kan bearbeta informationen, t.ex. genom att samköra den mot elektroniska uppgifter som har hämtats från andra informationskällor. Det ökar risken för att uppgifterna behandlas i strid med de grundläggande kraven på dataskydd. Utlämnande genom direktåtkomst brukar förknippas med särskilda risker för den personliga integriteten. En sådan risk är att uppgifterna sprids som en följd av att de upptagningar som direktåtkomsten avser blir allmänna handlingar hos den mottagande myndigheten (prop. 2017/18:269 s. 131). Direktåtkomst innebär också att uppgifter typiskt sett blir tillgängliga för fler personer i de verksamheter som har åtkomst och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar (Utlänningsdatalag, prop. 2015/16:65, s. 89 f.).

Viss sekretessreglering har införts för att minska de risker som ökat elektroniskt utlämnande medför. Enligt 11 kap. 4 § offentlighets- och sekretesslagen (2009:400) gäller att om en myndighet har elektronisk tillgång till en upptagning för automatiserad behandling hos en annan myndighet och en uppgift i denna upptagning är sekretessreglerad, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten.

11.1.2 Nuvarande möjligheter till elektroniskt utlämnande

I 2 kap. 20 § polisdatalagen (2010:361) föreskrivs att enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Bestämmelsen gäller för Säkerhetspolisen genom hänvisning i 6 kap. 4 § 7 polisdatalagen. Regeringen kan meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. Sådana föreskrifter finns i bl.a. 18 § polisdataförordningen (2010:1155).

I förarbetena till polisdatalagen konstaterar regeringen att en ordning som innebär informationsutbyte enbart genom manuell behandling skapar praktiska problem, eftersom brottsbekämpningen bedrivs dygnet runt. Uppgifter som en tjänsteman behöver omedelbart för att kunna utföra en tjänsteåtgärd måste vara lätt tillgängliga även utanför vanlig kontorstid. Därför infördes regler om direktåtkomst i polisdatalagen. Regeringen ansåg dock att det inte borde vara möjligt att medge direktåtkomst till personuppgifter som behandlas av Säkerhetspolisen, eftersom myndigheten behandlar särskilt känsliga uppgifter. Några skäl för att ge möjlighet till direktåtkomst till sådana personuppgifter framkom varken under det utredningsarbete som låg till grund för lagstiftningen eller under remissbehandlingen (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 178 f.). Säkerhetspolisen fick därför inte någon möjlighet att tillhandahålla personuppgifter genom direktåtkomst vid polisdatalagens tillkomst.

Sedan den 1 mars 2018 har Säkerhetspolisen dock enligt 6 kap. 11 a § polisdatalagen möjlighet att medge Försvarets radioanstalt och Försvarsmakten direktåtkomst till personuppgifter som gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att dessa myndigheter, inom ramen för myndighetsöverskridande samverkan, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Bestämmelsen tillkom för att effektivisera informationsutbytet inom ramen för Nationellt centrum för terrorhotbedömningar (Ett effektivare informationsutbyte vid Nationellt centrum för terrorhotbedömningar, prop. 2017/18:36).

11.1.3 Ett effektivare informationsutbyte är nödvändigt

Det största terrorhotet mot Sverige kommer enligt Säkerhetspolisen från våldsbejakande islamistiska grupper. Flera hundra personer har rest från Sverige till konfliktområden för att ansluta sig till al-Qaidainspirerade grupper eller till Daesh. De som rest till ett konfliktområde utomlands och tränat eller stridit för våldsfrämjande grupper har förvärvat förmågor och skapat kontakter med individer som kan hjälpa dem att begå terroristattentat eller radikalisera eller rekrytera andra efter hemkomsten. Sammantaget bedöms hotet från våldsbejakande islamister mot Sverige vara förhöjt.

Säkerhetspolisen har stora behov av att utbyta information med såväl andra myndigheter som utländska samarbetspartners. Utbytet sker i dag huvudsakligen manuellt, både i förhållande till svenska och utländska myndigheter. Begränsningarna när det gäller elektroniskt utlämnande medför att myndigheten måste delge operativ information antingen i pappersform eller elektroniskt i enskilda handlingar. Eftersom Säkerhetspolisen dagligen utbyter mellan 50 och 100 meddelanden med enbart andra staters underrättelse- och säkerhetstjänster innebär det en avsevärd begränsning. Information som andra myndigheter har behov av kommer enligt Säkerhetspolisen inte myndigheterna till del i den utsträckning som är önskvärd på grund av att sätten för utlämnande är ineffektiva och resurskrävande. Det finns därför risk att viktig och brådskande information inte når fram i tid.

Säkerhetspolisens behov av effektivare informationsutbyte har ökat markant under de senaste åren. Det politiska läget i Sverige och i omvärlden, med bl.a. omfattande flyktingströmmar och ett ständigt terrorhot, ställer nya krav på samarbete och effektivt informationsutbyte med både svenska och utländska myndigheter. Mot den bakgrunden finns det skäl att se över Säkerhetspolisens möjligheter till elektroniskt utlämnande av uppgifter.

11.2 Elektroniskt utlämnande på annat sätt än genom direktåtkomst

Regeringens förslag: Säkerhetspolisen ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast *Datainspektionen* yttrar sig i denna del och avstyrker förslaget. Utan en närmare analys av vilka effekter på den personliga integriteten som utvidgningen får eller kan få går det inte att avgöra om utvidgningen kan anses proportionerlig i förhållande till enskildas personliga integritet.

Skälen för regeringens förslag: Bestämmelsen i 2 kap. 20 § polisdatalagen om att bara enstaka personuppgifter får lämnas ut på medium för automatiserad behandling har kritiserats då den ansetts otidsenlig och i alltför hög grad begränsade möjligheten att utnyttja de fördelar som elektronisk kommunikation kan ge. Mot bl.a. den bakgrunden föreslog regeringen i propositionen Brottsdatalag – kompletterande lagstiftning att begränsningen till enstaka personuppgifter skulle tas bort och att personuppgifter ska få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt (prop. 2017/18:269 s. 134–136). Bestämmelsen finns i dag i 2 kap. 12 § polisens brottsdatalag. Det finns skäl att på liknande sätt överväga om Säkerhetspolisen bör ges större utrymme för elektroniskt utlämnande. Även om det i relativt stor utsträckning förekommer integritetskänsliga personuppgifter i Säkerhetspolisens verksamhet måste riskerna med att överföra sådana uppgifter elektroniskt vägas mot behovet av snabb och effektiv kommunikation. Sekretessbestämmelserna tillsammans med regleringen av personuppgiftsbehandling skyddar vidare enskilda mot att möjligheten att lämna ut personuppgifter elektroniskt missbrukas. Den som överväger att lämna ut personuppgifter, oavsett i vilken form det görs, måste alltid bedöma om sekretessregleringen lägger hinder i vägen och, om så inte är fallet, om regelverket för personuppgiftsbehandling gör det möjligt att lämna uppgifterna i elektronisk form. Mottagaren måste dessutom alltid ha rättslig grund för behandlingen och är även i övrigt skyldig att leva upp till de krav som finns i reglerna om personuppgiftsbehandling. Regeringen anser att regleringen, med dess krav för utlämnande och mottagande, är utformad på ett sätt som ger ett gott skydd för den personliga integriteten. Det finns inte skäl att vidare analysera utvidgningens effekter på det sätt som *Datainspektionen* efterfrågar. I den nya lagen bör det därför tas in en bestämmelse som ger Säkerhetspolisen möjlighet att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Samma uttryck som i polisens brottsdatalag bör användas.

Eftersom det i vissa fall kan vara svårare att göra en generell bedömning av om elektroniskt utlämnande kan vara lämpligt, bör det finnas utrymme för regeringen att meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Den närmare innebörden av vad som ska anses vara ett

olämpligt utlämnande får dock utvecklas genom tillsynsmyndighetens arbete och i domstolspraxis (jfr prop. 2017/18:269 s. 136).

11.3 Direktåtkomst

11.3.1 Behovet av direktåtkomst

Regeringens förslag: Elektroniskt utlämnande genom direktåtkomst ska vara tillåtet enbart i den utsträckning som anges i den nya lagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen av remissinstanserna har yttrat sig särskilt över behovet av direktåtkomst.

Skälen för regeringens förslag

Som framgår av avsnitt 11.1.2 såg lagstiftaren vid polisdatalagens tillkomst inte något behov av att reglera direktåtkomst till personuppgifter som Säkerhetspolisen behandlar. Någon egentlig analys av det lämpliga i att tillåta direktåtkomst gjordes inte (prop. 2009/10:85 s. 178 f.). Det är den tekniska utformningen av systemet som avgörande för om utlämnandet ska anses som direktåtkomst eller som annat utlämnande på medium för automatiserad behandling. Med hänsyn till att viss direktåtkomst till Säkerhetspolisens information har tillåtits inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning och att det har framkommit att Säkerhetspolisen har behov av att kunna dela information på ett helt annat sätt än tidigare har saken kommit i ett annat ljus. De tidigare förarbetsuttalandena hindrar därför inte att en annan bedömning görs nu.

Eftersom brottsbekämpning bedrivs dygnet runt är en ordning med i huvudsak manuellt utlämnande begränsande. Uppgifter som en tjänsteman behöver omedelbart för att kunna genomföra en tjänsteåtgärd måste vara tillgängliga även utanför kontorstid. Om så inte är fallet fördröjs informationsöverföringen, vilket kan få allvarliga konsekvenser för brottsbekämpningen. Det kan vidare ofta vara bråttom att hantera den information som kommer in till Säkerhetspolisen. Det kan t.ex. röra sig om information om ett planerat attentat mot mål i Sverige eller mot svenska intressen. Det är då viktigt att Säkerhetspolisen kan dela med sig av informationen till andra berörda myndigheter så fort som möjligt.

Genom direktåtkomst behöver den mottagande myndigheten inte vända sig till den utlämnande myndigheten med en särskild begäran utan tjänstemännen kan i stället eftersöka och hämta den information som direktåtkomsten ger tillgång till. Direktåtkomst medför dock att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar. En möjlighet till direktåtkomst anses därför, som framgår av avsnitt 11.1.1, generellt sett medföra ökad risk för intrång i den personliga integriteten. Säkerhetspolisen behandlar stora mängder personuppgifter i sina uppgiftssamlingar och många av dem är av känslig karaktär. Ju fler personer som har tillgång till sådana uppgiftssamlingar desto mer påtaglig

är risken för intrång. Även om det är möjligt att genom särskilda åtgärder motverka eventuella risker är det viktigt att mottagarnas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna. Verksamhetsbehoven måste därför vägas mot hänsynen till den enskildes integritet.

Säkerhetspolisen utbyter redan en stor mängd information med både nationella och utländska myndigheter. En möjlighet att medge direktåtkomst innebär inte att Säkerhetspolisen får behandla eller lämna ut fler eller andra personuppgifter än i dag. Det ligger också i sakens natur att Säkerhetspolisen lägger särskild vikt vid att pröva om information ska delas med andra. Myndigheten har ett starkt intresse av att se till att inte fler uppgifter än nödvändigt tillgängliggörs för andra. En möjlighet att medge direktåtkomst förändrar ingenting i det avseendet. Myndigheten har också redan i dag möjlighet att lämna ut uppgifter genom direktåtkomst till Försvarets radioanstalt och Försvarsmakten inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning. Mot denna bakgrund och då den utökade möjlighet att lämna ut personuppgifter elektroniskt som föreslås i avsnitt 11.2 i vissa fall inte bedöms räcka för Säkerhetspolisens informationslämnande, bör den nya lagen tillåta utlämnande genom direktåtkomst.

Enligt 2 kap. 21 § första stycket polisdatalagen, som genom en hänvisning i 6 kap. 4 § 7 gäller för Säkerhetspolisen, är utlämnande genom direktåtkomst tillåtet bara i den utsträckning som följer av lagen. I förarbetena till polisdatalagen framhålls att det från integritetssynpunkt finns fördelar med en lösning där det i lagen framgår i vilken utsträckning direktåtkomst får medges. Det underlättar för tillämparen om det anges i vilken utsträckning direktåtkomst får förekomma (prop. 2009/10:85 s. 172). En motsvarande bestämmelse bör därför införas i den nya lagen. Genom det säkerställs att riksdagen beslutar om i vilken utsträckning det är tillåtet att medge direktåtkomst.

11.3.2 Direktåtkomst för vissa svenska myndigheter

Regeringens förslag: Polismyndigheten ska för att kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller för att kunna fullgöra sina uppgifter enligt utlänningslagen eller lagen om särskild utlänningskontroll få medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar för vissa syften.

Försvarets radioanstalt ska i sin försvarsunderrättelseverksamhet få medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar för vissa syften. Detsamma ska gälla Försvarsmakten i dess försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Direktåtkomsten ska endast få avse personuppgifter som har gjorts gemensamt tillgängliga.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens förslag till direktåtkomst för Polismyndigheten omfattar inte personuppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen. Enligt förslaget får direktåtkomst

medges i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten hos både Försvarsmakten och Försvarets radioanstalt.

Remissinstanserna: *Datainspektionen* anser att riskerna och effekterna av att medge de aktuella myndigheterna direktåtkomst behöver utredas ytterligare och avstyrker därför förslaget. *Justitiekanslern* anser att det i betänkandet redovisas utförliga analyser både av behovet av att införa en möjlighet till direktåtkomst och det integritetsintrång det kan förväntas medföra. Det görs också tydliga överväganden kring säkerhetsåtgärder som minskar riskerna för den personliga integriteten och det finns inte skäl att invända mot den huvudsakliga intresseavvägningen som betänkandet presenterat. *Säkerhetspolisen* anser att möjligheten att medge Polismyndigheten direktåtkomst även bör omfatta personuppgifter enligt utlännings- och medborgarskapslagstiftningen. Myndigheten anser vidare att det bör tydliggöras om den föreslagna möjligheten att medge Försvarsmakten och Försvarets radioanstalt direktåtkomst även omfattar sådana uppgifter som regleras i 6 kap. 11 a § polisdatalagen. *Försvarets radioanstalt* påpekar att det bör tydliggöras att direktåtkomsten för myndigheten endast avser dess försvarsunderrättelseverksamhet.

Skälen för regeringens förslag

Direktåtkomst bara för några få myndigheter

De brottsbekämpande myndigheterna behöver samarbeta för att bekämpa brottslighet. Av samma skäl som det är viktigt att man inom Säkerhetspolisen på ett effektivt sätt kan tillgodogöra sig den information som samlats inom myndigheten är det viktigt att nyttiggöra informationen i samarbetet med andra brottsbekämpande myndigheter (jfr prop. 2009/10:85 s. 166 f.). Bland de brottsbekämpande myndigheterna är det dock enligt regeringens mening bara Polismyndigheten som har sådana arbetsuppgifter att det bör övervägas om Säkerhetspolisen ska kunna tillhandahålla information genom direktåtkomst.

Säkerhetspolisen samarbetar också nära med Försvarsmakten och Försvarets radioanstalt. Samarbetet är av stor betydelse för att Säkerhetspolisen ska kunna fullgöra sina uppgifter som säkerhetstjänst. Även i förhållande till dessa myndigheter bör det därför övervägas om Säkerhetspolisen, utöver det utbyte som redan sker inom ramen för Nationellt centrum för terrorhotbedömningar, ska kunna tillhandahålla information genom direktåtkomst.

För att Säkerhetspolisen på ett effektivt sätt ska kunna förebygga, förhindra och upptäcka brottslig verksamhet och utreda och lagföra brott krävs det ett utvecklat samarbete även med andra myndigheter. Säkerhetspolisen är initiativtagare och sammankallande i Samverkansrådet mot terrorism där 13 andra myndigheter ingår. Samarbetet syftar till att stärka Sveriges förmåga att motverka och hantera terrorism. Ett annat exempel är Säkerhetspolisens samarbete med Migrationsverket i syfte att identifiera säkerhetshot i migrationsströmmarna till Sverige. Liksom utredningen anser regeringen att det i dag inte finns något behov av att kunna medge någon av dessa myndigheter direktåtkomst.

Direktåtkomst för Polismyndigheten

Säkerhetspolisen och Polismyndigheten har ett väl utvecklat samarbete. Säkerhetspolisen ska enligt 11 § förordningen (2014:1103) med instruktion för Säkerhetspolisen samarbeta med Polismyndigheten i den utsträckning som behövs för att polisverksamheten ska kunna bedrivas effektivt. Ett effektivt samarbete kräver ett omfattande utbyte av information. Ett stort antal av de personer som Säkerhetspolisen har ögonen på är samtidigt föremål för underrättelseverksamhet eller brottsutredning hos Polismyndigheten på grund av att de misstänks för annan brottslighet. I Säkerhetspolisens brottsbekämpning kan inte sällan andra brott avslöjas. Information som rör allvarliga brott som har begåtts eller planeras bör naturligtvis kunna delas. Ett effektivt informationsutbyte mellan Säkerhetspolisen och Polismyndigheten är därför en förutsättning för att kunna förebygga och förhindra såväl terrorism som organiserad brottslighet. Myndigheterna kan vidare ha ett ömsesidigt intresse av att känna till om den andra myndigheten vill ha hjälp med iakttagelser rörande vissa personer. Likaså finns det ibland intresse av att se till att den andra myndigheten inte ingriper mot en viss person om ett obetydligt brott skulle begås, eftersom det skulle kunna skada pågående brottsspaning eller brottsutredning som rör allvarligare brott.

Informationsutbyte kan också vara helt avgörande för att kunna bedöma och reducera hot. I operativa ärenden är behovet av information dessutom tidskritiskt. Som exempel kan nämnas attentatet på Drottninggatan i Stockholm den 7 april 2017 och mordet på statsminister Olof Palme.

Regeringen delar utredningens bedömning att övervägande skäl talar för att Säkerhetspolisen bör ges möjlighet att medge Polismyndigheten direktåtkomst till personuppgifter som behandlas hos Säkerhetspolisen.

Direktåtkomst för Försvarets radioanstalt och Försvarsmakten

Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt har uppdrag som rör skyddet av Sveriges säkerhet och som förutsätter ett nära samarbete och kontinuerligt informationsutbyte. Försvarsmakten och Försvarets radioanstalt har möjlighet att medge Säkerhetspolisen direktåtkomst till vissa uppgiftssamlingar hos respektive myndighet. Vidare är Säkerhetspolisen en av de myndigheter som enligt 4 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får ange inriktning för Försvarets radioanstalts signalspaning.

Ett exempel på ett mer formaliserat samarbete mellan myndigheterna är samarbetet inom ramen för Nationellt centrum för terrorhotbedömning. Där arbetar myndigheterna tillsammans i gemensamma lokaler och tar gemensamt fram rapporter om terrorhotet mot Sverige och svenska intressen. Syftet är att stärka den samlade förmågan hos Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt och att ta tillvara myndigheternas samlade kompetens. Samarbetet kräver ett omfattande informationsutbyte. Sedan i mars 2018 har Säkerhetspolisen möjlighet att medge dessa myndigheter direktåtkomst till vissa uppgifter inom ramen för det samarbetet.

Myndigheternas behov av att utbyta information är emellertid inte begränsat till arbetet vid Nationellt centrum för terrorhotbedömning. Upp-

gifter som behandlas av en av myndigheterna kan tillsammans med uppgifter som behandlas av en annan ge en helhetsbild som inte framträder om bara den ena delen analyseras. Ett effektivt informationsutbyte kan alltså vara en förutsättning för att myndigheterna ska kunna fullgöra sina respektive uppdrag.

Mot den bakgrunden anser regeringen, liksom utredningen, att övervägande skäl talar för att Säkerhetspolisen bör ges möjlighet att medge Försvarets radioanstalt och Försvarsmakten direktåtkomst till personuppgifter som behandlas hos Säkerhetspolisen.

Hur bör direktåtkomsten avgränsas?

Direktåtkomst innebär att uppgifter som behandlas av Säkerhetspolisen blir tillgängliga utanför det sammanhang där de ursprungligen behandlades. Det är då ur ett integritetsperspektiv rimligt att de särskilda, mer begränsande, reglerna om gemensamt tillgängliga uppgifter alltid tillämpas. Direktåtkomst bör därför endast kunna medges till uppgifter som är gemensamt tillgängliga i Säkerhetspolisens verksamhet.

Från ett integritetsperspektiv är det en fördel om det tydligt framgår av författningstexten vilka uppgifter som får lämnas ut genom direktåtkomst. Några begränsningar av det slaget har emellertid inte ansetts möjliga att utforma inom annan brottsbekämpande verksamhet. De enda undantagen är direktåtkomsten till dna-register och fingeravtrycksregister, där de myndigheter som har direktåtkomst endast får veta om en person förekommer i registren. Det är, som utredningen framhåller, varken möjligt eller lämpligt att i den nya lagen begränsa vilken typ av uppgifter som direktåtkomsten får avse. Åtkomsten bör i stället begränsas till personuppgifter som Säkerhetspolisen behandlar med stöd av vissa rättsliga grunder.

När det gäller Försvarsmakten och Försvarets radioanstalt har Säkerhetspolisen främst behov av att dela information som behandlas inom områdena kontraterrorism, kontraspionage och författningsskydd. För Polismyndigheten är det främst uppgifter som rör kontraterrorism, kontraspionage, författningsskydd och personskydd som är av intresse. Sådana uppgifter kan ha betydelse för Polismyndighetens brottsbekämpande verksamhet, särskilt när det gäller underrättelseverksamheten och det brottsförebyggande arbetet, men även för brottsutredningar i enskilda fall. Direktåtkomst bör därför kunna medges till sådana uppgifter.

Säkerhetspolisen har påpekat att möjligheten att medge Polismyndigheten direktåtkomst även bör omfatta personuppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen. Säkerhetspolisen ska enligt 12 kap. 14 § andra stycket utlänningslagen (2005:716) verkställa beslut om avvisning eller utvisning i säkerhetsärenden. Migrationsverket eller den domstol som avgör ärendet får dock i beslutet om avvisning eller utvisning bestämma att en annan myndighet ska ombesörja verkställigheten. Den myndighet som i praktiken oftast kan komma i fråga i detta avseende är Polismyndigheten. Säkerhetspolisen kan därför ha behov av att utbyta information med Polismyndigheten angående verkställigheten av säkerhetsärenden. Även vid åtgärder enligt lagen (1991:572) om särskild utlänningskontroll kan

behov uppstå av informationsutbyte med Polismyndigheten. Direktåtkomst bör därför även omfatta uppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen.

De mottagande myndigheterna har vidare bara behov av att ta del av uppgifter från Säkerhetspolisen inom vissa delar av sin verksamhet. Polismyndighetens behov gör sig främst gällande i den brottsbekämpande verksamheten. Som *Säkerhetspolisen* påpekat har Polismyndigheten även behov av att ta del av uppgifter när myndigheten fullgöra uppgifter enligt utlänningslagen och lagen om särskild utlänningskontroll.

Försvarets radioanstalt framhåller att myndigheten enbart har behov av att ta del av information från Säkerhetspolisen genom direktåtkomst i sin försvarsunderrättelseverksamhet. Försvarsmakten har däremot behov av att ta del av information genom direktåtkomst i både försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Det bör framgå av bestämmelserna om direktåtkomst att direktåtkomst endast får medges för att vissa uppgifter ska kunna utföras eller för att användas i vissa verksamheter. På så sätt kan åtkomsten begränsas. Finns det behov av att begränsa omfattningen av direktåtkomsten ytterligare bör det göras i förordning eller i myndighetsinterna regler.

En annan fråga är hur direktåtkomsten bör avgränsas tekniskt. Ett alternativ är att direktåtkomst endast ges till en avskild uppgiftssamling som upprättats i syfte att dela information. Nackdelen med den lösningen är att det finns risk att de uppgifter som Säkerhetspolisen överför till uppgiftssamlingen inte uppdateras när uppgifterna uppdateras i verksamheten. Det kan därför vara lämpligare att medge direktåtkomst till viss information i Säkerhetspolisens it-system och i stället begränsa tillgången till informationen genom tilldelning av behörighet eller på annat sätt. Möjligheten att begränsa tillgången är i stort sett densamma oavsett vilken teknisk lösning som väljs. Bestämmelserna om direktåtkomst i den nya lagen bör mot den bakgrunden inte begränsas till en uppgiftssamling eller någon liknande teknisk lösning.

Det bör framgå av lagen att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Direktåtkomst inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning behöver inte regleras särskilt

Enligt 6 kap. 11 a § första stycket polisdatalagen har Säkerhetspolisen möjlighet att medge Försvarets radioanstalt och Försvarsmakten direktåtkomst inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning. Den möjlighet att medge Försvarets radioanstalt och Försvarsmakten direktåtkomst till uppgifter som behandlas inom bl.a. området kontraterrorism som nu föreslås omfattar uppgiftsutbytet inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning. Någon bestämmelse som motsvarar 6 kap. 11 a § första stycket polisdatalagen behövs därför inte i den nya lagen.

Enligt 6 kap. 11 a § andra stycket ansvarar en myndighet som har medgetts direktåtkomst för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sin arbetsuppgift. I 1 kap. 16 § lagen (2007:258) om behandling av personuppgifter i

Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och 1 kap. 16 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, föreskrivs motsvarande begränsning. Även i brottsdatalagen har det införts en generell bestämmelse om att tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen är tillämplig för Polismyndigheten. Att aktuella myndigheter är skyldiga att vid direktåtkomst begränsa tillgången till uppgifter är således redan reglerat. En bestämmelse som motsvarar 6 kap. 11 a § andra stycket behövs därför inte i den nya lagen.

Risken för integritetsintrång ska minimeras

Direktåtkomst innebär som nyss nämnts inte att fler eller andra personuppgifter får behandlas eller tillhandahållas. För att det ska vara acceptabelt att tillåta direktåtkomst måste det emellertid säkerställas att det finns ett tillfredsställande skydd för den personliga integriteten.

En första viktig aspekt är vilket sekretesskydd personuppgifterna har hos den mottagande myndigheten. Sekretessregleringen ger i princip samma skydd för uppgifter i den brottsbekämpande verksamheten och i försvarsunderrättelseverksamheten. Uppgifter hos Säkerhetspolisen omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen, dvs. utrikessekretess, försvarssekretess och sekretess till skydd för brottsbekämpning. Dessa sekretessbestämmelser gäller även hos Polismyndigheten, Försvarsmakten och Försvarets radioanstalt. Skyddet för enskildas personliga och ekonomiska förhållanden regleras i olika kapitel i offentlighets- och sekretesslagen för myndigheterna i fråga. För Säkerhetspolisen och Polismyndigheten finns reglerna i 35 kap. och 37 kap. offentlighets- och sekretesslagen, medan de för Försvarsmakten och Försvarets radioanstalt finns i 38 kap. Regleringen ger dock i princip samma skydd.

En annan viktig fråga är hur uppgifterna kommer att användas hos den mottagande myndigheten. Om kretsen av personer som får tillgång till uppgifterna kan begränsas är risken för integritetsintrång generellt sett mindre. Av respektive myndighets registerförfattning framgår att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Det är således endast de tjänstemän som har behov av uppgifterna som får ges tillgång till dem.

Informationssäkerheten hos den mottagande myndigheten är också en viktig fråga. Är den säkerheten hög, så att det kan garanteras att informationen endast når dem som har rätt till den, inger möjlighet till direktåtkomst mindre betänkligheter från integritetssynpunkt än vad som annars hade varit fallet (jfr prop. 2009/10:85 s. 176). Polismyndigheten, Försvarets radioanstalt och Försvarsmakten har generellt en mycket hög säkerhet när det gäller hantering av information.

I förarbetena till polisdatalagen framhålls att det i fråga om direktåtkomst bör vara den myndighet som ansvarar för datasystemen som avgör i vilken utsträckning en annan myndighet kan anses tillgodose kraven på tillräcklig säkerhet. Den som medger direktåtkomst ska kunna ha kontroll över att det egna datasystemet alltjämt har tillräcklig säkerhet även efter det att andra myndigheter fått tillgång till det (prop. 2009/10:85 s. 178).

Den närmare bedömningen av tekniska och andra förutsättningar för direktåtkomst bör därför göras av Säkerhetspolisen. Innan Säkerhetspolisen medger direktåtkomst bör myndigheten således försäkra sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå. Det kan exempelvis vara fråga om system för utlämnande av behörighet, loggning av transaktioner och annan intern kontroll. Säkerhetspolisen bör kunna ställa upp villkor som rör sådana frågor. Det kan regleras i förordning.

Datainspektionen anser att riskerna och effekterna av att ge aktuella myndigheter direktåtkomst behöver utredas ytterligare. Regeringen anser dock, i likhet med *Justitiekanslern*, att utredningen ingående analyserar både behovet av direktåtkomst och de ökade integritetsrisker som en möjlighet till direktåtkomst kan medföra och hur dessa kan motverkas genom reglering av annat slag, som bestämmelser om sekretess, tillgång till uppgifter, informationssäkerhet och en effektiv tillsyn. Mot den bakgrunden anser regeringen att Säkerhetspolisen bör få möjlighet att medge vissa svenska myndigheter direktåtkomst.

I avsnitt 11.4 behandlas frågan om hur sekretessregleringen förhåller sig till de föreslagna bestämmelserna om direktåtkomst.

11.3.3 Direktåtkomst för underrättelse- och säkerhetstjänster inom EU och EES

Regeringens förslag: Om det behövs för samarbetet mot terrorism ska Säkerhetspolisen få medge en underrättelse- eller säkerhetstjänst i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga och som behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Säkerhetspolisen underrätta regeringen.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att direktåtkomst ska ges till en avskild uppgiftssamling som upprättats i syfte att dela information med utländska mottagare.

Remissinstanserna: *Datainspektionen* avstyrker utredningens förslag av samma skäl som när det gäller möjligheten till direktåtkomst för svenska myndigheter. *Justitiekanslern* anser, som redovisas under direktåtkomst för svenska myndigheter, att det inte finns skäl att invända mot den intresseavvägning som gjorts i betänkandet. *Säkerhets- och integritetsskyddsnämnden* anför att man har förståelse för Säkerhetspolisens behov av att kunna effektivisera informationsutbytet genom direktåtkomst, men anser att det finns anledning att ytterligare analysera frågan hur de personuppgifter som genom direktåtkomst sprids till utländska mottagare skyddas. Enligt nämnden bör i vart fall en liknande reglering beträffande villkor som föreslås gentemot svenska myndigheter övervägas även för utländska mottagare. *Sveriges advokatsamfund* anser att svenska myndigheters möjlighet att utbyta underrättelseinformation och samarbeta med andra länders myndigheter i många fall är ett angeläget och berättigat

intresse, men att de svenska myndigheterna i sådana situationer inte kommer att ha någon insyn i eller kontroll över hur de personuppgifter behandlas hos de utländska myndigheterna och för vilka ändamål behandlingen egentligen sker. *Säkerhetspolisen* förordar att möjligheten till direktåtkomst görs utan villkoret att personuppgifterna ska behandlas i en avskild uppgiftssamling.

Skälen för utredningens förslag

Viss reglering av direktåtkomst för utländska myndigheter finns

Inom ramen för EU-samarbetet har olika lösningar skapats som ger möjligheter att överföra personuppgifter elektroniskt. Ett exempel är Schengen Information System (SIS), som regleras i lagen (2000:344) om Schengens informationssystem. Varje stat ansvarar för sin del av systemet och registrerar uppgifter som genom EU:s försorg är åtkomliga genom direktåtkomst i varje stat som är medlem i Schengensamarbetet. Inom ramen för samarbetet enligt Prümrådsbeslutet får medlemsstaterna medge varandra direktåtkomst till uppgifter i dna- och fingeravtrycksregister. Ett annat exempel är samarbetet med Europol. Europol ansvarar för olika databaser och uppgiftssamlingar och ger myndigheter i medlemsstaterna tillgång till vissa uppgiftssamlingar genom direktåtkomst. Införlivandet av CBE-direktivet ger brottsbekämpande myndigheter direktåtkomst till uppgifter i andra staters fordonsregister. Även brottsbekämpande myndigheters tillgång till uppgifter i EU:s viseringsdatabas (VIS) är exempel på direktåtkomst över gränserna.

Eftersom nationell säkerhet ligger utanför EU-samarbetet kan det inte förväntas att liknande lösningar kommer att finnas inom Säkerhetspolisens verksamhetsområde. För att möjliggöra direktåtkomst krävs därför en annan reglering. I avsnitt 11.3 konstaterar regeringen att den utökade möjligheten att lämna ut uppgifter elektroniskt som föreslås inte är tillräcklig för att tillgodose Säkerhetspolisens nuvarande behov. Säkerhetspolisen bör därför ges möjlighet att medge även utländska mottagare direktåtkomst.

Vem bör kunna medges direktåtkomst?

Den internationella utvecklingen på terrorområdet, den våldsbejakande islamismens alltmer globala karaktär och ambitioner och utvecklingen i Sverige har enligt Säkerhetspolisen sammantaget ökat behovet av nära samverkan med säkerhets- och underrättelsetjänster i andra stater på både strategisk, taktisk och operativ nivå (Ds 2016:31 s. 158). Att Säkerhetspolisen, utöver att motverka terrorism i Sverige, även ska bidra till att förhindra terrorism utomlands ligger inte bara i svenskt intresse utan följer också av internationella åtaganden. Ett väl fungerande samarbete med andra underrättelse- och säkerhetstjänster är därför en förutsättning för att Säkerhetspolisen ska kunna fullgöra sina arbetsuppgifter.

Vid risk för terroristattentat är snabbhet i informationsutbytet av avgörande betydelse för att undvika skador. På samma sätt som när det gäller informationsutbyte med svenska myndigheter finns det därför behov av att kunna dela viss information genom direktåtkomst med utländska

myndigheter. Det gäller framför allt andra staters underrättelse- och säkerhetstjänster.

Det ligger närmast till hands att tillåta informationsutbyte av nu aktuellt slag med de andra nordiska länderna. Även underrättelse- och säkerhetstjänster inom EU är viktiga samarbetsparter. Utöver de bilaterala kontakterna deltar Säkerhetspolisen i flera arbetsgrupper inom ramen för EU-samarbetet, i arbetet vid Europol och i det europeiska forumet Counterterrorism Group (CTG). Det nära samarbete som förekommer inom EU när det gäller bekämpning av terrorism och de kopplingar till Sverige som man har kunnat konstatera vid några av terroristattentaten i Europa under senare år gör därför enligt regeringens mening att en begränsning till enbart de nordiska länderna blir för snäv. Mot den bakgrunden bör möjligheten till direktåtkomst omfatta medlemsstater i EU och EES.

Regeringen anser alltså i likhet med utredningen att det i den nya lagen bör tas in en bestämmelse som möjliggör utlämnande genom direktåtkomst till underrättelse- och säkerhetstjänster inom EU och EES.

Hur bör direktåtkomsten avgränsas?

Direktåtkomst innebär att uppgifter som behandlas av Säkerhetspolisen blir tillgängliga utanför det sammanhang där de ursprungligen behandlades. Det är då ur ett integritetsperspektiv rimligt att de särskilda, mer begränsande reglerna om gemensamt tillgängliga uppgifter alltid tillämpas. På samma sätt som när det gäller direktåtkomst för Polismyndigheten, Försvarsmakten och Försvarets radioanstalt bör direktåtkomst därför bara kunna ges till uppgifter som har gjorts gemensamt tillgängliga.

Det är framför allt i samarbetet mot terrorism som det finns behov av att tillhandahålla information genom direktåtkomst. Direktåtkomsten för utländska underrättelse- och säkerhetstjänster bör därför begränsas till personuppgifter som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka terrorbrott eller utreda sådana brott och som behövs för samarbetet mot terrorism.

För att förhindra att utländska myndigheter får del av fler uppgifter än vad de behöver har utredningen föreslagit att direktåtkomsten för underrättelse- och säkerhetstjänster inom EU eller EES endast ska få ges till uppgifter i en avskild uppgiftssamling som Säkerhetspolisen har upprättat i direkt syfte att dela information med sina utländska motsvarigheter. *Säkerhetspolisen* anser att det sätter upp onödiga och arbetskrävande begränsningar som inte kan motiveras av integritetsskäl.

Innan Säkerhetspolisen tillhandahåller personuppgifter till utländska myndigheter är Säkerhetspolisen skyldig att pröva dels om det finns sakliga skäl att låta en utländsk underrättelse- eller säkerhetstjänst få del av uppgifterna, dels de rättsliga förutsättningarna för att lämna ut dem. I det ingår att en sekretessprövning görs, om det inte finns någon sekretessbrytande bestämmelse som är tillämplig. Det gäller oavsett på vilket sätt uppgifterna tillhandahålls. När det konstaterats att uppgifterna kan lämnas ut kan de göras tillgängliga för direktåtkomst. Den faktiska tillgången till dem kan sedan begränsas genom tilldelning av behörigheter eller på annat sätt. Mot den bakgrunden anser regeringen att det inte bör

krävas att direktåtkomsten för utländska mottagare begränsas till personuppgifter som behandlas i en avskild uppgiftssamling

I avsnitt 11.4 behandlas frågan om hur sekretessregleringen förhåller sig till den föreslagna bestämmelsen om direktåtkomst.

Risken för integritetsintrång ska minimeras

En bestämmelse om direktåtkomst anger endast i vilken form uppgifterna får lämnas ut och innebär inte att andra uppgifter än de som i dag får lämnas ut kommer att lämnas ut. Det är viktigt att komma ihåg att det är fråga om en möjlighet för Säkerhetspolisen att medge en utländsk myndighet direktåtkomst, inte någon rätt för mottagaren att få sådan åtkomst. På samma sätt som vid annat utlämnande är det Säkerhetspolisen som avgör vilka uppgifter som ska tillgängliggöras för direktåtkomst.

Både *Säkerhets- och integritetsskyddsnämnden* och *Sveriges advokatsamfund* har haft synpunkter på hur de personuppgifter som genom direktåtkomst tillgängliggörs för utländska myndigheter ska skyddas. När personuppgifter lämnas ut till utländska myndigheter för behandling där kan det inte sällan vara svårt att avgöra vilket skydd uppgifterna får. Det gäller emellertid inte om utlämnandet begränsas till underrättelse- och säkerhetstjänster inom EU och EES. Där är regleringen av personuppgiftsbehandling och skyddet för personuppgifter, som utredningen framhåller, till stor del detsamma, eftersom alla stater är bundna av dataskyddskonventionen. För EU:s medlemsstater gäller även andra rättsakter som skapar en enhetlig reglering. Som *Säkerhets- och integritetsskyddsnämnden* framhåller bör Säkerhetspolisen också, på samma sätt som när det gäller möjlighet till direktåtkomst för svenska myndigheter, försäkra sig om att den utländska mottagaren har en acceptabel säkerhetsnivå innan direktåtkomst medges. Säkerhetspolisen bör även kunna ställa upp villkor som rör sådana frågor. Det kan regleras i förordning.

Det är särskilt viktigt att ett beslut att medge en utländsk myndighet direktåtkomst föregås av noggranna överväganden. För att säkerställa att sådana överväganden görs och att det lämpliga i att en annan stats myndighet genom direktåtkomst får del av vissa uppgifter noga övervägs, bör det i den nya lagen tas in en bestämmelse som föreskriver att Säkerhetspolisen, innan direktåtkomst medges första gången, ska underrätta regeringen. En sådan underrättelse ger regeringen möjlighet att, om det skulle visa sig vara nödvändigt, kunna utfärda närmare föreskrifter om direktåtkomsten.

Datainspektionen anser även när det gäller direktåtkomst för utländska mottagare att riskerna och effekterna av att medge direktåtkomst behöver utredas ytterligare. Regeringen anser dock i likhet med *Justitiekanslern* att utredningen ingående analyserar både behovet av direktåtkomst och de ökade integritetsrisker som en möjlighet till direktåtkomst kan medföra och hur dessa kan motverkas genom reglering av annat slag, som bestämmelser om underrättelseskyldighet och informationssäkerhet. Mot den bakgrunden anser regeringen att Säkerhetspolisen bör få möjlighet att medge utländska underrättelse- och säkerhetstjänster direktåtkomst.

11.4 Sekretessbrytande bestämmelser

11.4.1 Varför behövs sekretessbrytande bestämmelser?

Sekretess hos Säkerhetspolisen

De personuppgifter som Säkerhetspolisen behandlar omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400). Där regleras utrikes- och försvarssekretessen och sekretessen till skydd för brottsbekämpningen. Bestämmelserna är tillämpliga på uppgifter som hänför sig till eller rör viss verksamhet. Det innebär att de gäller i all verksamhet där sådana uppgifter förekommer.

Uppgifter om enskilda i Säkerhetspolisens verksamhet omfattas som regel av sekretess enligt 35 kap. 1 § offentlighets- och sekretesslagen. Enligt paragrafen gäller sekretess för uppgifter som rör enskildas personliga och ekonomiska förhållanden och som förekommer i verksamhet för att bl.a. förebygga brott. Uppgifter om enskilda kan även omfattas av sekretess enligt 37 kap. 1 § och 21 kap. 3 och 5 §§. Enligt 37 kap. 1 § gäller sekretess i verksamhet för kontroll över utlänningar och i ärenden om svenskt medborgarskap. Enligt 21 kap. 3 § gäller sekretess för enskildas kontaktuppgifter i vissa situationer och enligt 5 § gäller sekretess till skydd för utlännings säkerhet i vissa fall.

Sekretess mellan myndigheter

Ansvaret för brottsbekämpningen är uppdelat mellan flera myndigheter. Säkerhetspolisen har också uppdrag som angränsar till Försvarsmaktens och Försvarets radioanstalt när det gäller Sveriges säkerhet. Sekretess gäller i större eller mindre utsträckning för åtskilliga av de personuppgifter som behandlas inom dessa verksamheter. Enligt 8 kap. 1 § offentlighets- och sekretesslagen får uppgifter för vilka sekretess gäller inte röjas för andra myndigheter, om inte annat framgår av lagen eller lag eller förordning till vilken lagen hänvisar. När uppgifter ska lämnas mellan myndigheter måste därför hänsyn tas till sekretesslagstiftningen. Motsvarande begränsning gäller vid uppgiftslämnande mellan olika verksamhetsgrenar inom en myndighet, när dessa är att betrakta som självständiga i förhållande till varandra.

Offentlighets- och sekretesslagen innehåller bestämmelser som möjliggör utbyte av uppgifter mellan myndigheter utan hinder av sekretess. Av 10 kap. 2 § offentlighets- och sekretesslagen framgår att sekretessbelagda uppgifter får lämnas från en myndighet till en annan om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen, som är avsedd att tillämpas restriktivt, medger inte sekretessgenombrott på den grunden att den mottagande myndigheten behöver uppgifterna i sin verksamhet. Enligt 10 kap. 28 § första stycket hindrar sekretess inte att uppgifter lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Vidare kan uppgifter, med vissa undantag, lämnas ut med stöd av 10 kap. 19–26 §§, när uppgifterna behövs för olika i paragraferna angivna ändamål inom brottsbekämpningen, bl.a. förundersökning. Enligt den s.k. generalklausulen i 10 kap. 27 § gäller som huvudregel att en uppgift får lämnas ut till en

annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.

I 35 kap. 10 § offentlighets- och sekretesslagen föreskrivs att en uppgift, utan hinder av sekretessen i 35 kap. 1 §, får lämnas ut enligt vad som föreskrivs i bl.a. polisens brottsdatalag. I 2 kap. 7–11 §§ polisens brottsdatalag finns bestämmelser om att uppgifter får lämnas ut.

Förhållandet mellan direktåtkomst och sekretess

En bestämmelse om direktåtkomst reglerar endast tillåtligheten av ett visst tillvägagångssätt för att lämna ut uppgifter. En sådan bestämmelse har alltså inte någon självständig sekretessbrytande effekt; den är inte att se som en uppgiftsskyldighet enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen (Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling, prop. 2004/05:164, s. 83 och Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt, prop. 2006/07:46, s. 80). Möjligheterna för t.ex. en myndighet att vid informationsutbyte med en annan myndighet överföra uppgifter genom att medge den senare direktåtkomst till uppgifter som behandlas automatiserat begränsas därför inte sällan av sekretess. Eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – den vill ta del av, blir uppgifterna att anse som utlämnade i och med att direktåtkomst medges. Det spelar ingen roll om den mottagande myndigheten faktiskt tar del av en viss uppgift eller inte. En myndighet kan därför inte tillåta en annan myndighet direktåtkomst till uppgifter som, vid en sekretessprövning, den senare myndigheten inte med säkerhet skulle ha rätt att ta del av (Utökat elektroniskt informationsutbyte, prop. 2007/08:160, s. 73). Direktåtkomst förutsätter därför att det är fråga om offentliga uppgifter, uppgifter som omfattas av en bestämmelse om uppgiftsskyldighet eller att det finns en annan sekretessbrytande bestämmelse som gör att uppgiften kan lämnas ut (prop. 2009/10:85 s. 189 f.) I flera av de brottsbekämpande myndigheternas registerförfattningar finns det därför sekretessbrytande bestämmelser vid direktåtkomst.

11.4.2 Sekretessbrytande bestämmelser gentemot svenska myndigheter

Regeringens förslag: Polismyndigheten ska, trots viss sekretess enligt offentlighets- och sekretesslagen, ha rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften, om Polismyndigheten behöver uppgifterna för brottsbekämpning eller lagföring eller för att fullgöra uppgifter enligt utlänningslagen eller lagen om särskild utlänningskontroll.

Försvarsmakten ska, trots viss sekretess enligt offentlighets- och sekretesslagen, ha rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften, om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst. Detsamma gäller

för Försvarets radioanstalt om myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Då utredningen inte föreslår att direktåtkomsten för Polismyndigheten ska omfatta personuppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen finns det inte med i den sekretessbrytande bestämmelsen för Polismyndigheten.

Remissinstanserna: *Datainspektionen* avstyrker förslaget då myndigheten anser att Polismyndigheten, Försvarets radioanstalt och Försvarsmakten inte ska medges direktåtkomst till uppgifter som Säkerhetspolisen behandlar. Det finns därmed inte skäl att utöka rätten för myndigheterna att ta del av uppgifter via föreslaget sekretessgenombrott. *Säkerhetspolisen* påpekar att den sekretessbrytande bestämmelsen för Polismyndigheten bör justeras så att den även omfattar personuppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen.

Skälen för utredningens förslag

Sekretessen måste brytas

I avsnitt 11.3.2 föreslås att Säkerhetspolisen ska ges möjlighet att lämna ut personuppgifter till Polismyndigheten, Försvarets radioanstalt och Försvarsmakten genom direktåtkomst. Eftersom de uppgifter som Säkerhetspolisen behandlar i sin brottsbekämpande verksamhet som regel omfattas av sekretess behövs det bestämmelser som bryter sekretessen för att utlämnandet genom direktåtkomst ska bli effektivt. I annat fall måste det göras en sekretessprövning i varje enskilt fall innan uppgifterna görs tillgängliga för direktåtkomst.

Offentlighets- och sekretesslagen innehåller flera sekretessbrytande bestämmelser. Som framgår av avsnitt 11.4.1 reglerar en bestämmelse om direktåtkomst endast själva formen för utlämnandet, dvs. på vilket sätt uppgifterna får lämnas ut, och är inte en sådan uppgiftsskyldighet som har sekretessbrytande verkan enligt 10 kap. 28 §. Bestämmelser om direktåtkomst brukar därför ofta kompletteras med sekretessbrytande bestämmelser som är utformade som uppgiftsskyldigheter på det sätt som avses i 10 kap. 28 §. Det bör därför tas in sådana bestämmelser i den nya lagen för att utlämnandet genom direktåtkomst ska bli effektivt

I dag finns i 6 kap. 11 b § polisdatalagen en sekretessbrytande bestämmelse som ger Försvarets radioanstalt och Försvarsmakten rätt att ta del av uppgifter som gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning. Uppgiftsskyldigheten gäller dock bara inom ramen för det samarbetet. En motsvarande bestämmelse bör därför inte införas i den nya lagen.

Bestämmelser om uppgiftsskyldighet

Sekretessbrytande bestämmelser i form av uppgiftsskyldighet brukar formuleras som en rätt för mottagaren att ta del av vissa uppgifter. Så har bestämmelserna om uppgiftsskyldighet formulerats i övriga registerförfattningar. Den formuleringen bör därför användas i den nya lagen.

Uppgiftsskyldigheten bör omfatta sådana uppgifter som de mottagande myndigheterna får ta del av genom direktåtkomst (avsnitt 11.3.2). Det innebär som *Säkerhetspolisen* påpekar att även uppgifter som behandlas för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen bör omfattas. De mottagande myndigheterna bör dessutom bara få tillgång till de aktuella uppgifterna när de behöver det för att kunna utföra vissa av sina arbetsuppgifter. För Polismyndigheten gäller det uppgifter som behövs för brottsbekämpning, lagföring eller för att fullgöra uppgifter som myndigheten har enligt utlänningslagen eller lagen om särskild utlänningskontroll. För Försvarsmakten är det uppgifter som myndigheten behöver i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst och för Försvarets radioanstalt uppgifter som myndigheten behöver i sin försvarsunderrättelseverksamhet. Det bör framgå av bestämmelserna.

Vilka sekretessbestämmelser ska den nya regleringen avse?

Frågan är vilken slags sekretess som behöver brytas för att Säkerhetspolisen ska kunna lämna ut uppgifter genom direktåtkomst. Bestämmelserna i 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen avser att skydda nationens intressen och den verksamhet som Säkerhetspolisen bedriver. Enligt regeringens mening bör det inte medföra någon fara för rikets säkerhet eller innebära någon skada för Säkerhetspolisens verksamhet eller för nationen att sådana uppgifter som Säkerhetspolisen anser bör göras tillgängliga för Polismyndigheten, Försvarsmakten och Försvarets radioanstalt lämnas ut till dessa myndigheter. Skaderekvisitet är då inte uppfyllt och något generellt behov av att bryta sekretessen enligt dessa bestämmelser kan inte anses föreligga. I de fall där utlämnandet av en uppgift till någon av de aktuella myndigheterna skulle innebära att Säkerhetspolisens egen verksamhet riskerar att skadas, bör direktåtkomst givetvis inte komma ifråga.

Regeringen gör samma bedömning i fråga om uppgifter som omfattas av sekretess enligt 21 kap. 5 § offentlighets- och sekretesslagen. Den sekretessen gäller till skydd för utlännings säkerhet i vissa fall. Sekretess gäller om det kan antas att röjande av uppgiften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållandet mellan utlänningen och en utländsk stat eller myndighet eller organisation av utlänningar. Uppgiftslämnande till de angivna myndigheterna bör inte medföra någon sådan fara för enskilda. Bestämmelsen är dessutom tillämplig hos de mottagande myndigheterna. Det finns därför inget behov av att bryta sekretessen enligt den paragrafen.

Uppgifter om enskildas personliga och ekonomiska förhållanden omfattas hos Säkerhetspolisen av sekretess enligt 21 kap. 3 §, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen. Utlämnande av sådana uppgifter torde nästan alltid anses vara till skada eller men för den enskilde. När sådana uppgifter ska lämnas ut måste dessutom en sekretessprövning göras i varje enskilt fall. Det är inte möjligt att på förhand göra en generell intresseavvägning beträffande sådana uppgifter. För att Säkerhetspolisen ska kunna lämna ut den typen av uppgifter till Polismyndigheten, Försvarsmakten och Försvarets radioanstalt genom direktåtkomst krävs det därför att sekretessen bryts.

Bestämmelserna om sekretess till skydd för enskilda i 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen gäller även i Polismyndighetens verksamhet. För Försvarsmakten och Försvarets radioanstalt finns en motsvarande bestämmelse om sekretess till skydd för enskilda i 38 kap. 4 §. Samtliga nu angivna bestämmelser gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men. Sekretesskyddet för uppgifter om enskilda ser således i princip likadant ut för de aktuella myndigheterna. Bestämmelsen i 21 kap. 3 § är tillämplig i hela den statliga förvaltningen och gäller således hos alla myndigheter.

Bestämmelserna om uppgiftsskyldighet gentemot Polismyndigheten, Försvarets radioanstalt och Försvarsmakten bör således bryta den sekretess som gäller enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen. I den mån andra sekretessbestämmelser är tillämpliga får det, på samma sätt som nu, göras en bedömning i det enskilda fallet av om sekretessen hindrar att uppgifterna lämnas ut.

Den nu föreslagna regleringen innebär alltså att ett sekretessgenombrott ska tillåtas i vissa fall. Bestämmelsen om utlämnande måste emellertid ses tillsammans med hur regelsystemet i övrigt har byggts upp. För det första bör utlämnandet bara, som utredningen föreslår, få avse uppgifter som har gjorts gemensamt tillgängliga. Detta innebär i sig en begränsning, eftersom en del av de uppgifter som Säkerhetspolisen behandlar aldrig kommer att göras gemensamt tillgängliga. För behandlingen av gemensamt tillgängliga uppgifter ska, som framgår av avsnitt 10.1, gälla särskilda begränsningar, vilket bl.a. innebär att enligt huvudregeln bara vissa typer av uppgifter ska vara åtkomliga vid sökning. Om direktåtkomst beviljas, kommer dessutom tillgången till olika typer av uppgifter att begränsas genom behörighetsregler. När en uppgift blir åtkomlig för en tjänsteman vid en annan myndighet kommer den myndighetens registerförfattning – som i likhet med Säkerhetspolisens innehåller regler som syftar till att minska risken för integritetsintrång – att bli tillämpliga. Den sekretessbrytande regeln måste också ses tillsammans med bestämmelserna om att tillgången till personuppgifter ska begränsas till vad den enskilde tjänstemannen behöver för att fullgöra sina arbetsuppgifter. Till skillnad från *Datainspektionen* anser regeringen att förslaget skapar förutsättningar för bättre informationsutbyte mellan de aktuella myndigheterna, samtidigt som risken för integritetsintrång beaktas.

Det bör tydliggöras i lagen att regeringen, på motsvarande sätt som enligt lagen om polisens behandling av personuppgifter inom brottsdatalagens område, ska ha möjlighet att meddela föreskrifter om att uppgifter får lämnas ut även i andra fall än de som redovisats ovan.

11.4.3 Sekretessbrytande bestämmelser i övrigt

Regeringens förslag: Om det är förenligt med svenska intressen, ska personuppgifter få lämnas ut till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott. Om det

är förenligt med svenska intressen ska personuppgifter också få lämnas ut till en utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter ska vidare få lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Uppgifter som omfattas av sekretess får inte röjas för en utländsk myndighet. Lagstiftaren har dock föreskrivit undantag från denna huvudregel bl.a. om utlämnandet görs i enlighet med särskild föreskrift i lag eller förordning. Det framgår av 8 kap. 3 § 1 offentlighets- och sekretesslagen. En sådan föreskrift finns i 2 kap. 15 § polisdatalagen. Där regleras utlämnande av personuppgifter till utländska myndigheter och organ. Bestämmelsen gäller genom hänvisning i 6 kap. 4 § 6 i Säkerhetspolisens verksamhet. Om det är förenligt med svenska intressen får personuppgifter lämnas ut till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott. Om det är förenligt med svenska intressen får personuppgifter också lämnas ut till utländsk underrättelse- eller säkerhetstjänst. Personuppgifter får dessutom lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Säkerhets- och integritetsskyddsnämnden har vid en granskning uttalat sig om den bedömning som ska göras vid utlämnande med stöd av 2 kap. 15 § polisdatalagen. Nämnden hänvisar till förarbetena till den tidigare gällande sekretesslagen (1980:100), där det anges att det intresse som sekretessen ska skydda ska tas med i bedömningen av om ett utlämnande kan anses förenligt med svenska intressen. Nämnden konstaterar att Säkerhetspolisens behov av att lämna uppgifter alltid måste vägas mot sekretessintresset, t.ex. det integritetsintrång och de konsekvenser som det kan innebära för den enskilde, vid bedömningen av om känslig underrättelseinformation kan lämnas till utlandet (se uttalande den 22 maj 2013, dnr 205–2012 s. 3).

Säkerhetspolisen bör kunna lämna ut uppgifter till en utländsk myndighet eller mellanfolklig organisation i samma utsträckning som i dag. En bestämmelse om det bör därför tas in i den nya lagen. Det innebär att Säkerhetspolisen, innan uppgifter görs tillgängliga för direktåtkomst, måste pröva om utlämnandet är förenligt med svenska intressen.

Det bör påpekas att när Säkerhetspolisen lämnar personuppgifter till mottagare i tredjeland eller till internationella organisationer måste myndigheten se till att utlämnandet är förenligt med bestämmelserna om överföring till sådana mottagare (avsnitt 17.3 och 17.4).

11.4.4 Uppgiftsskyldighet när det gäller rättsstatistik

Regeringens förslag: Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Enligt 2 kap. 14 § polisdatalagen ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för att framställa sådan statistik. Bestämmelsen gäller för Säkerhetspolisen genom en hänvisning i 6 kap. 4 § 6 polisdatalagen. Enligt 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet är rådet statistikansvarig myndighet. Av 24 kap. 8 § första stycket offentlighets- och sekretesslagen gäller absolut sekretess för uppgifter om en enskilds personliga och ekonomiska förhållanden i sådan särskild verksamhet hos en myndighet som avser framställning av statistik.

Skyldigheten att lämna uppgifter till rättsstatistiken regleras numera i 2 kap. 21 § brottsdatalagen. En motsvarande bestämmelse bör finnas i den nya lagen.

12 Längsta tid som personuppgifter får behandlas

12.1 Struktur och terminologi i den nya lagen

Regeringens förslag: Bestämmelser som motsvarar befintliga bestämmelser i polisdatalagen om bevarande och gallring ska tas in i den nya lagen. De ska formuleras så att det tydligt framgår att det är fråga om dataskyddsbestämmelser.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Kammarrätten i Stockholm* påpekar att de olika tidsfristerna för hur länge personuppgifter får behandlas är mycket svåröverskådliga och att det skulle vara bra om det gick att hitta ett mer enhetligt system. *Riksarkivet* ser positivt på att terminologin på området renodlas så att begreppen bevarande och gallring endast används i arkivlagens (1990:782) mening. Riksarkivet välkomnar att det slås fast att regleringen inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar.

Skälen för regeringens förslag

Olika typer av bestämmelser

Enligt huvudregeln i 6 kap. 6 § första stycket polisdatalagen (2010:361) får personuppgifter som Säkerhetspolisen behandlar inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som

anges i kapitlet. Därutöver finns det i 6 kap. polisdatalagen ytterligare två typer av bestämmelser om bevarande och gallring av personuppgifter. De gäller enbart personuppgifter som behandlas automatiserat.

Den ena typen är bestämmelser om gallring och finns i 6 kap. 7 och 12 §§. De gäller för personuppgifter som inte förekommer i ärenden om utredning av eller lagföring för brott. Regleringen innebär att personuppgifterna inte får behandlas automatiserat efter vissa i lagen angivna tidsfrister. De får alltså inte heller som utgångspunkt arkiveras digitalt. Det följer av att det i 2 kap. 2 § andra stycket polisdatalagen görs undantag från 8 § andra stycket personuppgiftslagen (1998:204), som föreskriver att arkivlagstiftningen har företräde framför personuppgiftslagstiftningen. Bestämmelsen gäller för Säkerhetspolisen genom en hänvisning i 6 kap. 4 § 1. Behandling för arkivändamål är dock tillåten om det med stöd av 6 kap. 7 § tredje stycket eller 6 kap. 14 § har meddelats föreskrifter om att personuppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Den andra typen av bestämmelser begränsar möjligheten att behandla personuppgifter i myndighetens brottsbekämpande verksamhet. De finns i 6 kap. 13 § polisdatalagen, som hänvisar till 3 kap. 9–13 §§ samma lag. Bestämmelserna gäller för personuppgifter som har gjorts gemensamt tillgängliga i ärenden om utredning av eller lagföring för brott. De föreskriver hur länge personuppgifterna får behandlas i den brottsbekämpande verksamheten men det hindrar inte, till skillnad från bestämmelserna om gallring, att handlingarna arkiveras digitalt enligt arkivlagens bestämmelser. När behandling inte längre är tillåten för brottsbekämpande ändamål kan bevarande således ske för arkivändamål utan att det krävs särskilda föreskrifter om det.

I 6 kap. 6 § tredje stycket upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om digital arkivering och om att vissa kategorier av personuppgifter får behandlas i den brottsbekämpande verksamheten under längre tid än vad som annars är föreskrivet. Sådana föreskrifter finns i 20–26 §§ polisdataförordningen (2010:1155). Av 19 § framgår att personuppgifter som arkiveras digitalt ska avskiljas från den brottsbekämpande verksamheten och att åtkomst till uppgifterna ska begränsas på visst sätt.

Regleringen bör samlas i ett särskilt kapitel

Bestämmelser som reglerar hur länge personuppgifter får behandlas är viktiga för att skydda den personliga integriteten. Det bör därför tas in bestämmelser i den nya lagen som motsvarar regleringen i polisdatalagen om hur länge olika typer av personuppgifter får behandlas. De bör samlas i ett särskilt kapitel för att ge tillämparen bättre överblick över hur länge personuppgifter får behandlas enligt lagen. Samma lösning har valts i övriga registerförfattningar (Brottsdatalag – kompletterande lagstiftning, prop. 2017/18:269, s. 121).

Bestämmelserna om bevarande och gallring är dataskyddsbestämmelser

Utgångspunkten i det arkivrättsliga regelverket är att uppgifter ska bevaras, medan presumtionen i regelverk som skyddar personuppgifter är den

omvända. Gallring enligt det arkivrättsliga regelverket syftar till att begränsa arkivens omfattning bland annat för att därmed öka deras tillgänglighet, medan gallring enligt registerförfattningarna syftar till att skydda enskildas personliga integritet (se exempelvis Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 207 f. och Tullbrottsdatalagen, prop. 2016/17:91, s. 169). I de brottsbekämpande myndigheternas registerförfattningar har terminologin renodlats för att så långt möjligt skilja mellan arkivrättsliga regler och regler om dataskydd. Orden bevarande och gallring används där enbart i den betydelse de har i arkivlagstiftningen. När syftet med bestämmelserna är att skydda den personliga integriteten anges i stället den yttersta gränsen för hur länge personuppgifterna får behandlas. Det gäller både i bestämmelser som motsvarar de nuvarande gallringsbestämmelserna och i bestämmelser som begränsar möjligheten att behandla personuppgifter i den brottsbekämpande verksamheten (prop. 2017/18:269 s. 120 f.). Regeringen har där även bemött *Kammarrätten i Stockholms* synpunkter på att regleringen är svåröverskådlig.

Regleringen i den nya lagen bör utformas på motsvarande sätt och bestämmelserna formuleras så att de genomgående anger den längsta tid uppgifterna får behandlas. Avsikten är dock inte att den ändrade terminologin ska föranleda några ändringar i sak.

12.2 Hur länge får personuppgifter behandlas?

12.2.1 Den längsta tid som personuppgifter får behandlas

Regeringens förslag: Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Utredningens förslag: överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Säkerhetspolisen* anför att prövningen hur länge personuppgifterna får behandlas bör göras mot de ändamål för vilka uppgifterna behandlas, inte mot syftena som utredningen föreslår. Myndigheten anser vidare att rekvisitet nödvändigt ska ersättas med behövs. *Riksarkivet* anser att det i fråga om lämplig skyddsåtgärd för att skydda den enskildes integritet vid arkivering inte alltid är säkrare med arkivering på papper än elektronisk sådan. Riksarkivet bedömer också att integritetskänsliga personuppgifter som huvudregel inte bör gallras och att sådana uppgifter i stället bör skyddas genom bestämmelser om sekretess och informationssäker behandling av uppgifterna.

Skälen för regeringens förslag

Personuppgifter får bara behandlas så länge de behövs för ändamål inom lagens tillämpningsområde.

Enligt huvudregeln i 6 kap. 6 § första stycket polisdatalagen får personuppgifter inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i kapitlet. En motsvarande bestämmelse

bör tas in i den nya lagen. För att tydliggöra att det inte är fråga om bevarande i arkivlagens mening bör ordet behandlas användas i stället för bevaras. Som *Säkerhetspolisen* anser bör bestämmelsen utformas på samma sätt som bestämmelsen i 2 kap. 17 § brottsdatalagen och utgå från ändamålet med behandlingen i stället för syftena. Av de skäl som anges i avsnitt 8.3.1 bör ordet nödvändigt användas i stället för behövs. Säkerhetspolisen bör alltså inte få behandla personuppgifter under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Om Säkerhetspolisen behandlar en personuppgift för flera ändamål samtidigt varierar tiden för hur länge uppgiften behöver behandlas. Att det inte längre finns behov av att behandla personuppgiften för ett visst ändamål medför inte att behandlingen av den måste upphöra för alla andra ändamål samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål inte att den får fortsätta att behandlas för alla ändamål lika länge.

Liksom i polisdatalagen bör bestämmelsen kompletteras med mer detaljerade bestämmelser om hur länge vissa kategorier av personuppgifter får behandlas. Regeringen återkommer till det.

Behandling för arkivändamål

Enligt 8 § andra stycket personuppgiftslagen hindrar bestämmelserna i lagen inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Arkivlagstiftningen har alltså i fråga om allmänna handlingar företräde framför personuppgiftslagens bestämmelser om längsta bevarandetid. För att tydliggöra att personuppgifter får arkiveras när de inte längre behövs för något av de tillåtna ändamålen bör det tas in en bestämmelse i den nya lagen som motsvarar 8 § andra stycket personuppgiftslagen. I vilken utsträckning personuppgifterna ska gallras regleras i det arkivrättsliga regelverket.

För Säkerhetspolisens del görs i polisdatalagen undantag från 8 § andra stycket personuppgiftslagen när det gäller personuppgifter som ska gallras enligt polisdatalagen. Syftet med regleringen är som nyss nämnts att förtydliga att personuppgifter i dessa fall inte får behandlas automatiserat för arkivändamål, det vill säga att uppgifterna inte får arkiveras digitalt. Uppgifterna får dock behandlas för arkivändamål om de överförs till pappersform. För att tydliggöra att ingen förändring i det avseendet är avsedd, trots den ändrade terminologin, bör ett motsvarande undantag som i polisdatalagen göras i den nya lagen. Vad gäller *Riksarkivets* framförda synpunkter om arkivering på papper och fördelarna med elektronisk sådan hänvisas till vad regeringen anfört i förarbetena till de brottsbekämpande myndigheternas registerförfattningar (prop. 2017/18:269 s. 124).

Det bör anmärkas att behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde, oavsett om det är Säkerhetspolisen som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet (Brottsdatalag, prop. 2017/18:232, s. 167).

12.2.2 Personuppgifter som inte har gjorts gemensamt tillgängliga

Regeringens förslag: Personuppgifter som inte har gjorts gemensamt tillgängliga ska inte få behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, och inte längre än ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 6 kap 7 § första stycket polisdatalagen föreskrivs att personuppgifter som behandlas automatiserat av Säkerhetspolisen och som inte har gjorts gemensamt tillgängliga ska gallras senast ett år efter det att ärendet avslutades, om de behandlas i ett ärende. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången. Regeringen delar utredningens uppfattning att det inte finns skäl att ändra på hur länge sådana uppgifter får behandlas. En motsvarande bestämmelse bör därför tas in i den nya lagen, men den bör reglera hur länge personuppgifterna får behandlas.

Av 2 kap. 2 § andra stycket polisdatalagen följer att arkivlagstiftningen inte ska ha företräde om 6 kap. 7 § är tillämplig. Syftet med regleringen är att förtydliga att personuppgifter i dessa fall inte får behandlas automatiserat för arkivändamål. Det bör gälla även enligt den nya lagen. Det bör således göras undantag från bestämmelsen om att arkivlagstiftningen ska ha företräde (avsnitt 12.2.1).

Den nu föreslagna regleringen bör inte gälla personuppgifter i ärenden om utredning av eller lagföring för brott. Den frågan behandlas i avsnitt 12.2.5.

12.2.3 Personuppgifter som har gjorts gemensamt tillgängliga

Regeringens förslag: Personuppgifter som har gjorts gemensamt tillgängliga ska som huvudregel inte få behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år ska dock inte få behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge. Det förutsätter att någon ny registrering inte har gjorts efter det att han eller hon fyllt 18 år.

Personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information ska inte få behandlas längre än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att endast sådana omständigheter som har betydelse för

personens anknytning till brottslig verksamhet bör kunna påverka längsta tid för behandling av personuppgifter i underrättelseverksamhet.

Remissinstanserna: *Datainspektionen* tillstyrker förslaget att införa begränsande regler för hur länge uppgifter om personer under 18 år får behandlas. Datainspektionen tillstyrker vidare utredningens förslag att endast uppgifter om en persons anknytning till brottslig verksamhet ska påverka längsta tid för behandling av personuppgifter i underrättelseverksamhet. *Säkerhetspolisen* anser däremot att bestämmelsen inte är ändamålsenlig vid personuppgiftsbehandling i myndighetens underrättelseverksamhet. *Säkerhets- och integritetsskyddsnämnden* anser att det är angeläget att det tydliggörs om en ny registrering avseende en person förlänger tiden för behandling enbart avseende den personen, eller om registreringen även påverkar tiden för behandling avseende personer som har anknytning till samma brottsliga verksamhet.

Skälen för regeringens förslag

Gemensamt tillgängliga personuppgifter ska som huvudregel få behandlas lika länge som i dag

Enligt 6 kap. 12 § polisdatalagen ska gemensamt tillgängliga personuppgifter gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

I förarbetena till polisdatalagen gjordes bedömningen att en allmän gallringsfrist om tio år utgjorde en lämplig avvägning mellan Säkerhetspolisens behov och den enskildes krav på att uppgifter inte bevaras alltför lång tid. I fråga om personuppgifter som förekommer i en uppgiftssamling som skapats för att bearbeta och analysera information gjordes dock bedömningen att en kortare gallringsfrist borde gälla (prop. 2009/10:85 s. 269). Den bedömning som gjordes då av hur länge personuppgifter bör få behandlas har enligt regeringens mening fortfarande fog för sig. Bestämmelserna bör av de skäl som anges i avsnitt 12.1.1 formuleras så att de anger hur länge uppgifterna får behandlas. Regeringen återkommer till behovet av att beträffande några kategorier av personuppgifter ha en mer differentierad reglering.

Av 2 kap. 2 § andra stycket polisdatalagen följer att arkivlagstiftningen inte ska ha företräde om 6 kap. 12 § är tillämplig. Detsamma bör gälla enligt den nya lagen. Det bör därför göras undantag från den föreslagna regeln om att arkivlagstiftningen ska ha företräde för nu aktuella personuppgifter.

En särskild bestämmelse för personuppgifter som rör barn

Polisdatalagen innehåller inte några särskilda bestämmelser om behandling av personuppgifter som avser barn. Samma bestämmelser gäller således vid personuppgiftsbehandlingen oavsett den registrerades ålder. Säkerhetspolisen har i sina interna styrdokument reglerat gallringsfristen i myndighetens centralregister för personer som vid tiden för registreringen inte fyllt 18 år. Sådana uppgifter gallras senast fem år efter det att en

uppgift om personen senast infördes. Säkerhets- och integritetsskyddsnämnden har särskilt granskat hur brottsbekämpande myndigheter behandlar personuppgifter om barn. Nämnden har uttalat att integritetsskyddande regler i polisdatalagen gör sig gällande i särskilt hög grad vid behandling av uppgifter om barn. Nämnden är också positiv till Säkerhetspolisens interna bestämmelser om kortare gallringsfrist för sådana uppgifter (uttalande den 17 februari 2016, dnr 50–2015 s. 5 och 8). Mot den bakgrunden anser regeringen i likhet med utredningen att det i den nya lagen bör föreskrivas kortare tid för behandling av uppgifter om personer som vid registreringen inte hade fyllt 18 år. Sådana uppgifter bör inte få behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen avseende den unge gjordes.

Omständigheter som kan påverka längsta tid för behandling i underrättelseverksamhet

I dag framgår det av 6 kap. 12 § polisdatalagen att den tid som personuppgifter får behandlas i underrättelseverksamhet kan förlängas om en ny registrering avseende personen i fråga görs. Det framgår emellertid inte av bestämmelsen vad den registrering som kan föranleda att personuppgifter får fortsätta att behandlas ska avse. Tiden för hur länge personuppgifter får behandlas ska naturligtvis inte kunna påverkas av vilka uppgifter som helst. I de brottsbekämpande myndigheternas registerförfattningar har motsvarande bestämmelser om hur länge personuppgifter får behandlas i underrättelseverksamhet därför förtydligats på så sätt att det endast är sådana omständigheter som har betydelse för personens anknytning till brottslig verksamhet som ska påverka hur länge personuppgifterna får behandlas (prop. 2017/18:269 s. 128 f.). Utredningen föreslår att samma förtydligande ska göras i den nya lagen.

Det är självfallet viktigt att vilka uppgifter som helst inte ska påverka hur länge personuppgifter får behandlas. Ett förtydligande i denna del hade därför varit önskvärt. När det gäller Säkerhetspolisens underrättelseverksamhet är det dock ofta svårt att veta vilken brottslig verksamhet en viss uppgift kan hänföras till eftersom myndigheten agerar i ett så tidigt skede. Om möjligheterna att fortsätta behandla personuppgifter knyts till omständigheter som har betydelse för personens anknytning till brottslig verksamhet kan det leda till att färre uppgifter än i dag påverkar hur länge personuppgifter får behandlas, vilket skulle vara negativt för Säkerhetspolisens underrättelseverksamhet. Det är heller inte möjligt att, inom ramen för detta lagstiftningsärende, finna en annan lösning som kan förtydliga vilka uppgifter som ska påverka längsta tid för behandling av uppgifter i underrättelseverksamheten. Mot den bakgrunden anser regeringen, till skillnad från *Datainspektionen* men i likhet med *Säkerhetspolisen*, att regleringen på samma sätt som i dag bör utgå från när den senaste registreringen avseende personen gjordes.

Säkerhets- och integritetsskyddsnämnden efterfrågar ett tydliggörande av om en ny registrering avseende en person kan förlänga tiden för behandling även för andra personer med anknytning till samma brottsliga verksamhet. Frågan är relevant trots att vilka uppgifter som kan förlänga registrering inte knyts till brottslig verksamhet. Det är inte uteslutet att en registrering avseende en person kan förlänga tiden för behandling även för

andra personer med anknytning till den personen. Till exempel kan misstankar mot en person innebära att misstankarna mot en annan person stärks, eftersom det tydliggör att båda har starka kopplingar till en viss plats, en viss annan person eller en viss företeelse. I vilka fall en ny registrering avseende en person ska påverka tiden för behandling avseende en annan person måste dock avgöras från fall till fall (jfr prop. 2017/18:269 s. 129).

12.2.4 Personuppgifter som rör viss säkerhetshotande verksamhet

Regeringens förslag: Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt ska inte få behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhetspolisen* anser att personuppgifter som rör säkerhetshotande verksamhet ska kunna behandlas som längst i 70 år på grund av den långsiktighet som präglar kontraspionageverksamheten. *Datainspektionen* avstyrker förslaget då utredningen inte visat att det finns ett behov av att spara uppgifterna under så lång tid.

Skälen för regeringens förslag

Vad är kontraspionage?

Säkerhetspolisens kontraspionageverksamhet har till uppgift att förebygga, förhindra och upptäcka spioneri, olaglig underrättelseverksamhet och andra brott mot Sveriges säkerhet. Kontraspionage omfattar inhämtning av underrättelser om och bedömning av andra staters spionage mot Sverige. Sådant underrättelsearbete skapar underlag för olika typer av åtgärder mot andra staters säkerhetshotande underrättelseverksamhet och är en del av Sveriges försvar.

Spioneribrott utövas ofta av två aktörer i förening. Den ena är en underrättelseofficer som tillhör en utländsk underrättelsetjänst. Den andra är spionen som t.ex. kan ha tillgång till information och miljöer där information kan inhämtas på uppdrag av underrättelseofficeren. Underrättelseofficerare arbetar långsiktigt med att leta efter lämpliga mål och att närma sig och odla kontakter med personer som har information om målet, för att i senare skeden eventuellt kunna rekrytera dem som spioner och handleda dem. Andra stater söker alltså fortlöpande efter lämpliga personer att rekrytera. Själva processen fram till värvningstillfället kan ta några år och i vissa fall ännu längre tid. I den efterföljande handledningsfasen kan den värvade personen handledas så länge han eller hon har tillgång eller kan få tillgång till den information som den andra statens underrättelsetjänst är intresserad av. Det kan pågå i flera decennier. En underrättelseofficer är däremot som regel bara stationerad i Sverige några år och förflyttas sedan till ett annat land. Eftersom stationeringstiden är

begränsad måste värvning och handledning av spioner lämnas över mellan underrättelseofficerare.

Säkerhetspolisen arbetar med två olika metoder för att identifiera spioner. En metod är att leta direkt efter dem. En annan är att kartlägga och följa utländska underrättelseofficerares aktiviteter för att kunna identifiera misstänkta spioner. Genom att underrättelseofficerare lämnar handledningen vidare till sina efterträdare innebär byte av underrättelseofficerare en möjlighet för Säkerhetspolisen att kunna identifiera misstänkta spioner. Det är emellertid svårt, eftersom underrättelseofficerare är tränade i att undvika värdlandets säkerhetstjänst. Det innebär att iakttagelser som görs beträffande en underrättelseofficer kanske inte byggs på med nya iakttagelser förrän efter flera byten på posten. Under tiden behöver informationen från kartläggningen behållas.

Andra staters underrättelseverksamhet i Sverige bygger således på långsiktigt arbete. En anledning till det är att det är relativt svårt att värva spioner. Det strävar därför efter att använda dem så länge som möjligt. Spioneri är oftast en livslång sysselsättning. Det finns också exempel både i Sverige och utomlands på att spioner rekryterar sina barn som spioner. Säkerhetspolisens kontraspionageverksamhet måste därför anpassas till det långsiktiga tidsperspektivet.

Oavsett vilken metod Säkerhetspolisen använder kräver kontraspionage lagring av information i flera decennier. Exempelvis använder Säkerhetspolisen i dag regelmässigt uppgifter som inhämtades på 1980- och 90-talen. Erfarenheter från både Sverige och andra länder visar att det ofta tar mycket lång tid innan en spion avslöjas. Spionerna Stig Wennerström och Arne Treholt kan nämnas som exempel på det.

Nuvarande bestämmelser är inte ändamålsenliga

Säkerhetspolisen har i dag möjlighet att behandla personuppgifter i sin brottsbekämpande verksamhet under relativt lång tid. Enligt 6 kap. 12 § första stycket polisdatalagen ska personuppgifter som gjorts gemensamt tillgängliga gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om det finns särskilda skäl får Säkerhetspolisen dock besluta att personuppgifter får bevaras längre, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Säkerhetspolisen kan således under vissa förutsättningar besluta att förlänga gallringsfristen för personuppgifter inom kontraspionaget med ytterligare tio år.

Säkerhetspolisen förlänger regelmässigt gallringsfristen för personuppgifter i kontraspionaget. Från den 1 januari 2017 till den 23 mars 2017 fattades enligt Säkerhetspolisen drygt 400 enskilda beslut om att förlänga gallringsfristen för personuppgifter som behandlas inom kontraspionaget. Det rör sig således om fler än tusen enskilda förlängningsbeslut per år. Hanteringen medför omfattande administrativt arbete för personal med särskild sakkunskap på området, eftersom lagstiftningen kräver att det fattas beslut om bevarande i varje enskilt fall.

Det finns risk för att personuppgifter, som borde bevaras, tas bort på grund av att Säkerhetspolisen i vissa fall måste prioritera operativa insatser före förlängningsbeslut. Inom kontraspionaget är det dessutom ofta svårt att vid tidpunkten för beslut om förlängning veta exakt vilka uppgifter som

kommer att behövas i framtiden. Förlängning av fristen kan inte beslutas retroaktivt. Säkerhetspolisen har uppgett att myndigheten i ett flertal fall har gallrat personuppgifter där det i efterhand har visat sig att informationen varit relevant och därför borde ha behandlats längre.

Uppgifter inom kontraspionaget ska få behandlas längre

På grund av kontraspionagets särdrag finns det alltså enligt regeringens mening behov av att behandla personuppgifter hänförliga till sådan verksamhet under betydligt längre tid än vad huvudregeln i polisdatalagen medger. Säkerhetspolisen har visserligen möjlighet att genom särskilda beslut förlänga tiden för behandling. Det är emellertid inte rimligt att lägga betydande resurser på att regelbundet fatta beslut om sådan förlängning när det ofta på förhand kan förutses att förlängning av fristen är nödvändig. Risken för att behandlingen av uppgifter upphör på grund av tidsbrist eller felaktiga beslut bör också vägas in. Mot den bakgrunden anser regeringen att Säkerhetspolisen bör få behandla personuppgifter hänförliga till området kontraspionage under längre tid än vad som är tillåtet i dag. Det gäller framför allt uppgifter där grunden för registreringen är att personen är en misstänkt utländsk underrättelseofficer och uppgifter om hans eller hennes närmaste anhöriga. Det gäller också uppgifter om misstänkta spioner och deras närmaste anhöriga och händelser kopplade till dessa personer. Om sådana personuppgifter får behandlas under längre tid skulle det ge Säkerhetspolisen större möjligheter att inte bara identifiera misstänkta spioner och underrättelseofficerare, utan också att avföra eventuella felaktiga misstankar. På så sätt kan en förlängd tidsfrist i det här fallet också till viss del stärka integritetsskyddet.

Frågan är hur tidsfristen för behandling av aktuella uppgifter bör bestämmas. Från integritetssynpunkt är det viktigt att personuppgifter inte behandlas för länge. Samtidigt måste tidsfristen bestämmas på ett sätt som är ändamålsenligt och tillgodoser de behov som finns.

Försvarssekretessen, som regleras i 15 kap. 2 § offentlighets- och sekretesslagen (2009:400), gäller enligt 4 § offentlighets- och sekretessförordningen (2009:641) i 95 år om uppgifterna rör underrättelseverksamheten inom underrättelse- och säkerhetstjänsten. Den svenska militära underrättelsetjänstens arbete och källor skyddas således under lång tid och man skulle kunna argumentera för att Säkerhetspolisens uppgifter som rör kontraspionage borde kunna behandlas lika länge. En annan möjlighet är att utgå från hur länge sekretess gäller för uppgifter i brottsbekämpande verksamhet, vilket är 70 år. En så lång tidsfrist som någon av de nu nämnda skulle dock innebära betydligt större integritetsintrång än i dag och markant förlänga tiden för hur länge personuppgifter för denna typ av verksamhet får behandlas. Att bestämma tidsfristen till 70 år som *Säkerhetspolisen* föreslår är därför inte aktuellt.

Erfarenheterna har visat att spioneri under 30–40 år inte är ovanligt. Med beaktande av det anser regeringen att fristen för hur länge personuppgifter i kontraspionageverksamheten ska få behandlas inte bör vara kortare än 40 år. Behandlingen av personuppgifterna kan då fortgå under en tid som motsvarar en spions yrkesverksamma liv. Med hänsyn till att det är fråga om mycket allvarliga brott anser regeringen att den föreslagna

tidsfristen är en rimlig avvägning mellan samhällsintressena och enskildas integritet.

Datainspektionen anser att utredningen inte har visat att det finns ett behov av att spara uppgifter under så lång tid som nu föreslås. Inspektionen anser också att riskerna för den enskildes personliga integritet inte har analyserats i tillräcklig utsträckning. Tiden för behandling av uppgifter i kontraspionageverksamheten förlängs som nyss nämnts regelmässigt. Förslaget innebär därför inte någon större skillnad mot den ordning som redan i dag gäller. Regeringen anser vidare att utredningen gör en tillräcklig analys av riskerna för enskildas personliga integritet. Det bör således i den nya lagen tas in en bestämmelse som föreskriver att personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt inte får behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Undantag bör göras för uppgifter som behandlas i en uppgiftssamling för bearbetning och analys. För sådana uppgifter bör tidsfristen om tre år gälla (avsnitt 12.2.3).

12.2.5 Ärenden om utredning av eller lagföring för brott

Regeringens förslag: Bestämmelser om begränsningar i möjligheten att behandla gemensamt tillgängliga uppgifter i brottsanmälningar, avslutade förundersökningar och andra liknande utredningar ska tas in i den nya lagen. Det ska framgå av bestämmelserna att de endast begränsar behandling för ändamål inom lagens tillämpningsområde.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering

I 3 kap. 10–12 §§ polisdatalagen regleras hur länge personuppgifter som har gjorts gemensamt tillgängliga i ärenden om utredning av eller lagföring för brott längst får behandlas automatiserat i den brottsbekämpande verksamheten. Där föreskrivs bl.a. att om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i den brottsbekämpande verksamheten. När det gäller förundersökningar och andra liknande utredningar föreskrivs att personuppgifter inte får behandlas i den brottsbekämpande verksamheten när det har förflutit fem år efter utgången av det kalenderår då en dom, eller ett beslut med anledning av domstolsprövning, vann laga kraft eller sedan fem år förflutit från utgången av det kalenderår då förundersökningen lades ned eller avslutades på annat sätt. I 3 kap. 13 § föreskrivs att om en förundersökning har lagts ned, om åtal har lagts ned eller om frikännande dom som har vunnit laga kraft har meddelats, får personen inte vara sökbar som misstänkt. Bestämmelserna gäller genom en hänvisning i 6 kap. 13 § polisdatalagen i Säkerhetspolisens verksamhet.

Samma reglering om längsta tid för behandling av personuppgifter som i dag

Bestämmelserna om längsta tid för behandling av personuppgifter i ärenden om utredning av och lagföring för brott är utförligt motiverade i förarbetena till polisdatalagen (prop. 2009/10:85 s. 223 f.). Skälen bakom den nuvarande ordningen gör sig fortfarande gällande. Det har inte heller framkommit skäl att ändra regelverket. Därför bör bestämmelser med motsvarande innehåll tas in i den nya lagen.

Bestämmelserna i 3 kap. 10 och 11 §§ polisdatalagen hindrar inte att personuppgifter som behandlas automatiserat i den brottsbekämpande verksamheten fortsätter att behandlas automatiserat för ändamål utanför lagens tillämpningsområde under längre tid än vad som anges i bestämmelserna. De inskränker alltså enbart behandling i den brottsbekämpande verksamheten, vilket innebär att personuppgifterna t.ex. får behandlas automatiserat för arkivändamål. För att tydliggöra det bör det framgå av bestämmelserna i den nya lagen att de enbart reglerar hur länge personuppgifter får behandlas för ändamål inom lagens tillämpningsområde.

12.2.6 Möjlighet att förlänga tiden för behandling

Regeringens förslag: Om det finns särskilda skäl och uppgifterna fortfarande behövs för det ändamål de behandlas för, ska Säkerhetspolisen få besluta att personuppgifter får behandlas under längre tid än vad som anges för en viss kategori av uppgifter. Om personuppgifter behandlas med stöd av ett sådant beslut ska frågan om fortsatt behandling prövas på nytt senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter i en uppgiftssamling som har skapats för att bearbeta och analysera information, senast vid utgången av det tredje kalenderåret efter beslutet. Tiden för behandling får vid varje tillfälle förlängas med längst samma tid som den ursprungliga eller, om uppgifterna rör säkerhetshotande verksamhet eller avser någon som är under 18 år, längst tio år.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Säkerhetspolisen har enligt 6 kap. 12 § tredje stycket polisdatalagen möjlighet att besluta att personuppgifter får bevaras längre än vad som anges i paragrafen, om det finns särskilda skäl och uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. För uppgifter som får bevaras längst tio år får tiden förlängas med tio år och för uppgifter som får bevaras längst tre år får tiden förlängas med tre år.

Säkerhetspolisen bör även fortsättningsvis ha möjlighet att i vissa fall besluta om förlängd tid för behandling. En motsvarande bestämmelse bör därför tas in i den nya lagen, men den bör formuleras så att den anger hur länge uppgifterna får behandlas i stället för hur länge de får bevaras.

På samma sätt som i dag bör Säkerhetspolisen, om det finns särskilda skäl, få förlänga fristen för behandling av uppgifter om personer som vid tiden för registreringen inte har fyllt 18 år med som längst tio år.

Regeringen instämmer vidare i utredningens bedömning att Säkerhetspolisen bör ges möjlighet att förlänga tidsfristen även för behandling av personuppgifter som rör viss säkerhetshotande verksamhet och som får behandlas längst 40 år. En förlängning motsvarande den tid som personuppgifterna ursprungligen får behandlas skulle dock i dessa fall leda till att uppgifterna får behandlas alltför länge. I likhet med vad som gäller för gemensamt tillgängliga uppgifter i övrigt bör uppgifterna få behandlas som längst tio år efter beslutet, om inte ett nytt beslut om förlängning fattas inom den fristen.

12.3 Rätt att meddela föreskrifter om längsta tid för behandling

Regeringens förslag: En upplysningsbestämmelse som motsvarar den befintliga bestämmelsen om rätt att meddela föreskrifter avseende fortsatt behandling av vissa kategorier av personuppgifter ska tas in i den nya lagen, men det ska förtydligas att den endast omfattar behandling av personuppgifter för ändamål inom tillämpningsområdet.

Det ska även i den nya lagen finnas en upplysningsbestämmelse om rätt att meddela föreskrifter avseende behandling av personuppgifter för vetenskapliga, statistiska eller historiska ändamål. Bestämmelsen ska formuleras så att det framgår att föreskriftsrätten även omfattar behandling för arkivändamål av allmänt intresse.

En upplysningsbestämmelse som motsvarar befintlig bestämmelse om rätt att meddela föreskrifter avseende digitalt arkiverade uppgifter ska tas in även i den nya lagen. Det ska dock förtydligas att bestämmelsen endast omfattar behandling av personuppgifter för ändamål inom tillämpningsområdet och att föreskriftsrätten avser begränsning av behandlingen av arkiverade uppgifter.

Utredningens förslag överensstämmer i huvudsak med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Föreskrifter om fortsatt behandling av vissa kategorier av personuppgifter

Enligt 3 kap. 12 § polisdatalagen, som genom en hänvisning i 6 kap. 13 § även gäller för Säkerhetspolisen, upplyses om att regeringen har möjlighet att meddela föreskrifter om att vissa kategorier av personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas i den brottsbekämpande verksamheten under längre tid än vad som anges i 3 kap. 10 och 11 §§. Skälen för regleringen är utförligt redovisade i förarbetena till polisdatalagen (prop. 2009/10:85 s. 226 f.). De gör sig alltjämt gällande och en motsvarande bestämmelse som upplyser om rätt att meddela föreskrifter bör därför tas in i den nya lagen.

Föreskrifter om fortsatt behandling av uppgifter för historiska, statistiska eller vetenskapliga ändamål

Regeringen eller den myndighet som regeringen bestämmer har enligt 6 kap. 7 § tredje stycket och 14 § polisdatalagen möjlighet att meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Motsvarande bestämmelse som upplyser om att regeringen kan meddela föreskrifter bör finnas i den nya lagen. Bestämmelsen bör dock formuleras om så att föreskriftsrätten avser hur länge personuppgifterna får behandlas. För att terminologin ska motsvara dataskyddsförordningens och registerförfattningarna inom brottsdatalagens tillämpningsområde bör det vidare framgå att föreskriftsrätten även omfattar behandling för arkivändamål av allmänt intresse (jfr prop. 2017/18:269 s. 124 f.).

Föreskrifter om användning av digitalt arkiverade uppgifter

Regeringen eller den myndighet som regeringen bestämmer har enligt 6 kap. 6 § tredje stycket polisdatalagen möjlighet att meddela föreskrifter om digital arkivering. I 19 § polisdataförordningen föreskrivs att personuppgifterna ska avskiljas från myndighetens brottsbekämpande verksamhet vid digital arkivering. Syftet är att uppgifterna inte ska vara digitalt åtkomliga i den verksamheten. Det ska alltså inte vara möjligt för vem som helst att enkelt söka fram de digitalt arkiverade personuppgifterna. Normalt bör det bara vara arkivarier som förfogar över uppgifterna och kan göra sökningar i dem. Brottsanmälningar, förundersökningar och andra brottsutredningar bör få behandlas för arkivändamål med stöd av arkivlagen trots att de inte längre får behandlas i den brottsbekämpande verksamheten.

Med hänsyn till att arkivlagen inte hindrar eller ställer upp några begränsningar för fortsatt automatiserad behandling av arkiverade uppgifter finns det även i fortsättningen behov av att kunna meddela föreskrifter till skydd för den personliga integriteten vid digital arkivering. En bestämmelse motsvarande den i 6 kap 6 § tredje stycket polisdatalagen bör därför tas in i den nya lagen. Det bör dock tydliggöras att föreskriftsrätten avser begränsningar av den behandling som sker av arkiverade uppgifter inom lagens tillämpningsområde (jfr prop. 2017/18:269 s. 127 f.).

13 Personuppgiftsansvar

13.1 Vad innebär personuppgiftsansvar?

13.1.1 Vem är personuppgiftsansvarig?

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

Säkerhetspolisen ska vara personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför. Polismyndigheten ska vara personuppgiftsansvarig för den behandling som myndigheten utför.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Personuppgiftsansvar är ett centralt begrepp i dataskyddslagstiftningen. Utgångspunkten är att det alltid ska finnas någon som bär ansvaret för att dataskyddsreglerna följs vid behandling av personuppgifter och som den enskilde kan vända sig till för att göra sina rättigheter gällande. Den personuppgiftsansvarige har det ansvaret. Det bör därför definieras vad som avses med personuppgiftsansvarig.

I brottsdatalagen definieras personuppgiftsansvarig som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Med hänsyn till att definitionen innehåller uttrycket behörig myndighet bör i stället den definition som finns i 3 § personuppgiftslagen (1998:204) och som genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen (2010:361) gäller för Säkerhetspolisen användas. Personuppgiftsansvarig bör därför definieras som den som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för behandlingen av personuppgifter.

Även om det definieras vad som avses med personuppgiftsansvarig bör det av den nya lagen tydligt framgå vem som är personuppgiftsansvarig. I 6 kap. 5 § första stycket polisdatalagen anges att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Det bör även gälla enligt den nya lagen. Eftersom Polismyndigheten i vissa fall ska tillämpa lagen bör den myndigheten vara personuppgiftsansvarig för den behandling som myndigheten utför enligt lagen.

13.1.2 Personuppgiftsansvarets omfattning

Regeringens förslag: Personuppgiftsansvaret ska omfatta all behandling av personuppgifter som utförs under respektive myndighets ledning eller på dess vägnar.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Av den nya lagen ska det framgå vad Säkerhetspolisen respektive Polismyndigheten i egenskap av personuppgiftsansvarig är skyldig att göra i olika situationer, t.ex. samarbeta med tillsynsmyndigheten, vidta säkerhetsåtgärder och utse dataskyddsombud. Detta bör regleras i ett särskilt kapitel i lagen som även omfattar personuppgiftsbiträden och deras skyldigheter.

I 3 kap. 1 § brottsdatalagen (2018:1177) föreskrivs att den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. Det bör även i den nya lagen klargöras hur långt personuppgiftsansvaret sträcker sig. På så sätt tydliggörs att den personuppgiftsansvarige har ett helhetsansvar genom att

personuppgiftsansvaret omfattar dels den personuppgiftsbehandling som förekommer vid myndigheten, dels den personuppgiftsbehandling som ett personuppgiftsbiträde utför på myndighetens vägnar. Den personuppgiftsansvariges helhetsansvar får också betydelse för det skadeståndsrättsliga ansvaret (avsnitt 16.3).

Det är myndigheten som är personuppgiftsansvarig, inte chefen eller någon anställd. Ytterst är det dock respektive myndighetschef som bär ansvaret för hur personuppgifter behandlas. Den omständigheten att det har utsetts ett dataskyddsombud påverkar inte personuppgiftsansvaret, eftersom dataskyddsombud inte har något ansvar för personuppgiftsbehandlingen (avsnitt 13.3).

13.1.3 Ingen reglering av gemensamt personuppgiftsansvar

Regeringens bedömning: Den nya lagen bör inte innehålla någon särskild bestämmelse om gemensamt personuppgiftsansvar.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att Säkerhetspolisen ska få vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Remissinstanserna: Ingen av remissinstanserna har yttrat sig särskilt över förslaget.

Skälen för regeringens bedömning

Personuppgiftsansvarig definieras sedan länge som den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen. En sådan definition föreslås som nyss nämnts även i den nya lagen. Två eller flera personuppgiftsansvariga kan därför vara gemensamt personuppgiftsansvariga för viss behandling.

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

Även om gemensamt personuppgiftsansvar mellan myndigheter är tillåtet, torde det i praktiken vara ovanligt. I de allra flesta fall är den personuppgiftsbehandling som förekommer väl avgränsad och går att härleda till en viss myndighet. Ibland förekommer det dock att flera myndigheter är ansvariga för samma behandling, om samarbetet innebär att de deltagande myndigheterna tillsammans bestämmer exempelvis vilka

uppgifter som ska samlas in, lagras eller tas bort. Gemensamt personuppgiftsansvar kan också de facto uppstå vid behandling av personuppgifter i en viss situation eller på ett visst sätt. Det finns omständigheter som talar för att ett gemensamt personuppgiftsansvar skulle kunna finnas för delar av den behandling av personuppgifter som sker inom ramen för arbetet vid Nationellt centrum för terrorhotbedömningar där Säkerhetspolisens deltar. Regeringen konstatera i förarbetena till den aktuella lagstiftningen att de deltagande myndigheter är väl medvetna om vad som innefattas i deras respektive personuppgiftsansvar och hur detta ansvar i praktiken ska utövas och avgränsas mellan myndigheterna. Det konstateras också att det är i rättstillämpningen som frågan om personuppgiftsansvarets fördelning slutligen avgörs (Ett effektivare informationsutbyte vid Nationellt centrum för terrorhotbedömningar, prop. 2017/18:36, s. 16–19).

Utredningen föreslår att det i den nya lagen ska tas in en bestämmelse som föreskriver att två eller flera behöriga myndigheter får vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning, eller om regeringen i enskilda fall beslutar om det. Ordningen för när gemensamt personuppgiftsansvar uppkommer skulle därmed, enligt utredningen, bli tydligare eftersom sådant ansvar då inte kan uppstå de facto i en viss situation, utan endast i den utsträckning som riksdagen eller regeringen har beslutat om det. Ett motsvarande förslag lämnade utredningen i sitt delbetänkande Brottsdatalag (SOU 2017:29).

I förarbetena till brottsdatalagen konstaterar regeringen dock att det i dataskyddsdirektivet föreskrivs att två eller flera personuppgiftsansvariga som gemensamt fastställer ändamålen med och medlen för behandlingen är gemensamt personuppgiftsansvariga. Någon motsvarighet till utredningens förslag finns inte i direktivet. Inte heller i dataskyddsförordningen finns något motsvarande formkrav för att ett gemensamt personuppgiftsansvar ska uppstå. Skillnaden mellan lydelsen i direktivet och lydelsen i utredningens förslag skulle därför kunna medföra att ett gemensamt personuppgiftsansvar i vissa fall föreligger enligt direktivet men inte enligt brottsdatalagen, vilket kan leda till oklarheter vid rättstillämpningen. Trots fördelarna med utredningens förslag, ansåg regeringen att bestämmelsen i brottsdatalagen skulle motsvara direktivets lydelse (prop. 2017/18:232 s. 215). I 3 kap. 20 § brottsdatalagen föreskrivs därför att två eller flera myndigheter är gemensamt personuppgiftsansvariga om de gemensamt fastställer ändamålen med och medlen för personuppgiftsbehandlingen. Den registrerade får utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga. Motsvarande ordning gäller vid gemensamt personuppgiftsansvar enligt dataskyddsförordningen.

Eftersom det redan av definitionen av personuppgiftsansvarig följer att två eller flera kan vara gemensamt personuppgiftsansvariga, kan varken dataskyddsförordningen eller brottsdatalagen sägas innehåller något direkt förtydligande i denna del. Mot den bakgrunden finns det inte skäl att i den nya lagen göra ett sådant förtydligande. Gemensamt personuppgiftsansvar kan uppkomma utan en sådan bestämmelse. Gemensamt personuppgiftsansvar torde dessutom förekomma väldigt sällan i Säkerhetspolisens verksamhet. Det finns därför inte behov av att i den nya lagen införa någon bestämmelse motsvarande 3 kap. 20 § brottsdatalagen.

13.2 Säkerhetspolisens skyldigheter som personuppgiftsansvarig

13.2.1 Brottsdatalagens bestämmelser om personuppgiftsansvarigas skyldigheter bör tas in i den nya lagen

Regeringens förslag: I den nya lagen ska det tas in bestämmelser som i huvudsak motsvarar dem som finns i brottsdatalagen om den personuppgiftsansvariges skyldigheter.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering

Som personuppgiftsansvarig är Säkerhetspolisen skyldig att vidta en mängd åtgärder för att bl.a. säkerställa att personuppgiftsbehandlingen utförs författningsenligt och skydda personuppgifterna. Skyldigheterna regleras dels i personuppgiftslagen, dels i polisdatalagen.

I 30 och 31 §§ personuppgiftslagen finns det bestämmelser om säkerhetsåtgärder och krav vid anlitande av personuppgiftsbiträden och i 38–40 §§ regleras personuppgiftsombudens uppgifter. I 2 kap. 11 § polisdatalagen föreskrivs att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter och i 6 kap. 5 § andra stycket föreskrivs att Säkerhetspolisen ska utse ett eller flera personuppgiftsombud. Vidare ska Säkerhetspolisen enligt 2 § polisdataförordningen (2010:1155) i vissa situationer samråda med Datainspektionen och Säkerhets- och integritetsskyddsnämnden.

Regleringen i brottsdatalagen

I 3 kap. brottsdatalagen regleras de personuppgiftsansvarigas skyldigheter. Där ställs krav på olika åtgärder för att säkerställa författningsenlig personuppgiftsbehandling och lämplig säkerhetsnivå. Det föreskrivs också att ett eller flera dataskyddsombud ska utses och det regleras utförligt vilka arbetsuppgifter ombuden ska ha. Det finns även bestämmelser om vad som gäller vid anlitande av personuppgiftsbiträden och vilka skyldigheter sådana biträden har. Vidare ställs det krav på samarbete med tillsynsmyndigheten. Regeringen kan meddela föreskrifter om skyldigheter att föra register över behandlingar och skyldigheten att införa interna rutiner för anmälan av överträdelser.

Regleringen bör vara densamma som i brottsdatalagen

Flertalet av de skyldigheter som behöriga myndigheter har i egenskap av personuppgiftsansvariga enligt brottsdatalagen gäller redan för Säkerhetspolisen. Vissa bestämmelser har motsvarigheter i Säkerhetspolisens nuvarande reglering, men är mer detaljerade eller har en något annorlunda utformning i brottsdatalagen. En del bestämmelser har emellertid ingen motsvarighet i dagens reglering och innebär således nya skyldigheter.

Regeringen delar utredningens uppfattning att huvuddelen av bestämmelserna om personuppgiftsansvarigas skyldigheter i brottsdatalagen är av sådan karaktär att de även bör tillämpas av Säkerhetspolisen. Merparten av bestämmelserna i 3 kap. brottsdatalagen bör därför ha sin motsvarighet i den nya lagen. Nedan följer en redogörelse för vilka skyldigheter Säkerhetspolisen bör ha som personuppgiftsansvarig och vad de innebär.

13.2.2 Tekniska och organisatoriska åtgärder

Regeringens förslag: Säkerhetspolisen ska genom lämpliga tekniska och organisatoriska åtgärder säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

Säkerhetspolisen ska också genom lämpliga tekniska och organisatoriska åtgärder se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd). I automatiserade behandlingssystem ska det som regel inte vara möjligt att behandla andra personuppgifter än dem som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* invänder att dataskyddsdirektivet inte medger att kravet på dataskydd som standard begränsas till automatiserade behandlingssystem. Vidare anser inspektionen att uppräkningen i artikel 20.2 dataskyddsdirektivet bör tas in i lagen. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Lämpliga tekniska och organisatoriska åtgärder ska vidtas

I 3 kap. 2 § brottsdatalagen föreskrivs att den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder, ska säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Bestämmelserna om tekniska och organisatoriska åtgärder saknar motsvarighet i 1995 års dataskyddsdirektiv och i personuppgiftslagen. I 31 § personuppgiftslagen finns dock bestämmelser om säkerhetsåtgärder.

Regeringen delar utredningens uppfattning att det bör ställas samma krav på Säkerhetspolisen som på övriga brottsbekämpande myndigheter. Det bör därför tas in en bestämmelse med samma innehåll som 3 kap. 2 § brottsdatalagen i den nya lagen. På samma sätt som när det gäller brottsdatalagen är det inte möjligt att i lagen ange vilka tekniska och organisatoriska åtgärder som bör vidtas. Det får avgöras i varje enskilt fall. Vilka omständigheter som Säkerhetspolisen ska beakta vid beslut om åtgärder kan regleras i förordning. Vid den bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga de är. Även grunden för behandlingen och riskerna med den ska beaktas.

Inbyggt dataskydd

Enligt 3 kap. 3 § brottsdatalagen ska den personuppgiftsansvarige när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd). Begreppet inbyggt dataskydd innebär att integritetsfrågor ska påverka it-systemen från förstudie och kravställning via design och utveckling till användning och avveckling. Genom krav på att integritetsfrågor ska beaktas under hela tidsperioden kan säkerheten i systemen höjas och författningsenlig och korrekt behandling underlättas. En motsvarande bestämmelse bör tas in i den nya lagen.

Det är det inte möjligt att föreskriva vilka tekniska och organisatoriska åtgärder som Säkerhetspolisen bör vidta för att leva upp till principen om inbyggt dataskydd. Det får avgöras i varje enskilt fall beroende på vilken del av verksamheten det rör sig om och vilka personuppgifter som ska behandlas. Det handlar främst om åtgärder för att minimera mängden personuppgifter, begränsa åtkomsten till uppgifterna och på olika sätt skydda dem (jfr prop. 2017/18:232 s. 177 f.). Vilka omständigheter som ska beaktas vid beslut om sådana åtgärder kan regleras i förordning.

Dataskydd som standard

Enligt 3 kap. 4 § brottsdatalagen ska den personuppgiftsansvarige se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

Dataskydd som standard innebär att arbetsflödena i ett system automatiskt ska styra användaren mot ett integritetssäkert arbetssätt och att grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att i standardfallet säkerställa att så sker. Det bör i detta avseende ställas samma krav på Säkerhetspolisen som på övriga brottsbekämpande myndigheter. En motsvarande bestämmelse bör därför tas in i den nya lagen.

Säkerhetspolisen ska säkerställa dataskydd som standard oavsett vilken behandling eller vilka personuppgifter det rör sig om och utan hänsyn till vad åtgärderna kostar. Dataskydd som standard gäller i princip i alla system där personuppgifter behandlas, men det måste finnas visst utrymme för avsteg från huvudregeln i de fall där myndigheten inte har rätt att införa sådana åtgärder. Som exempel kan nämnas standardprogram som Word och Outlook, där användaren inte råder över de tekniska lösningarna. I förarbetena till brottsdatalagen konstaterar regeringen att de behöriga myndigheterna även måste kunna använda sådana system. Mot den bakgrunden gäller kravet på dataskydd som standard i brottsdatalagen endast i automatiserade behandlingssystem, vilket till skillnad från vad Datainspektionen anfört, inte ansågs oförenligt med direktivet (prop. 2017/18:232 s. 179). Denna ordning bör gälla även i den nya lagen. Vad som avses med automatiserade behandlingssystem behandlas i avsnitt 7.3.

Dataskydd som standard innebär att det som regel inte ska vara möjligt att behandla andra personuppgifter än de som är nödvändiga för varje

särskilt angivet ändamål med behandlingen. Som framgår av avsnitt 8.3 är det långtifrån alltid möjligt att i underrättelseverksamhet ange ändamålen för behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. Det innebär att ändamålet kanske till en början inte kan anges mer preciserat än till vilken verksamhetsområde en viss uppgift hör, exempelvis kontraterrorism. Ändamålet får sedan preciseras mer när det blir möjligt. Vilka krav på dataskydd som standard blir är på motsvarande sätt beroende av i vilket skede i en process som personuppgifter behandlas och i vilka system uppgifterna behandlas.

Även om kravet på dataskydd som standard endast gäller i automatiserade behandlingssystem måste Säkerhetspolisen säkerställa att även behandling i de standardprogram som används lever upp till de grundläggande kraven på behandling av personuppgifter.

Datainspektionen har hänvisat till den synpunkt som myndigheten lämnat i sitt remissvar över delbetänkandet Brottsdatalag (SOU 2017:29) om att uppräkningen i artikel 20.2 i dataskyddsdirektivet borde tas in i brottsdatalagen. Som anges i förarbetena till brottsdatalagen skulle en sådan uppräkning i lagen kunde riskera att låsa myndigheterna vid viss utformning av automatiserade behandlingssystem och direktivets uppräkning togs därför inte in i lagen (prop. 2017/18:232 s. 179). Det finns inte skäl att nu göra någon annan bedömning.

13.2.3 Loggning i automatiserade behandlingssystem

Regeringens förslag: Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning som det är särskilt föreskrivet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* avstyrker förslaget om att kravet på loggning ska begränsas till automatiserade behandlingssystem och anför att begränsningen riskerar att försämra skyddet för den enskildes personliga integritet i förhållande till nuvarande regelverk. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Nuvarande reglering

Som tidigare nämnts ställs krav på säkerhetsåtgärder i 31 § personuppgiftslagen. De anses även omfatta loggning och liknande åtgärder. Bestämmelsen gäller för Säkerhetspolisen (2 kap. 2 § första stycket 7 och 6 kap. 4 § 1 polisdatalagen). Av Datainspektionens allmänna råd om säkerhet för personuppgifter framgår att det, beroende på känsligheten hos personuppgifterna, bör finnas en behandlingshistorik (logg) som sparas viss tid så att åtkomsten till uppgifterna kan kontrolleras. Enligt råden bör en behandlingshistorik normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Historiken bör, beroende på hur känsliga personuppgifterna är, ange t.ex. läsning, ändring, utplåning eller kopiering av personuppgifter (Säkerhet

för personuppgifter, Datainspektionens allmänna råd, november 2008, s. 22).

Loggning ska ske i automatiserade behandlingssystem

Loggning är en säkerhetsåtgärd som innebär att behandlingshistorik sparas under en viss tid. Det är en teknisk funktion i systemet som fungerar automatiskt och som inte går att ändra eller påverka på annat sätt. Loggning fyller flera olika funktioner. Den ger den personuppgiftsansvarige information både om hur behandlingssystemen används och om externa och interna angrepp mot systemen. Loggning är således mycket viktig för det interna säkerhetsarbetet. Den ger också tillsynsmyndigheten nödvändig information för granskning i efterhand av hur personuppgifter har behandlats. I 3 kap. 5 § brottsdatalagen finns därför en bestämmelse som slår fast att det krävs loggning. En motsvarande bestämmelse bör tas in i Säkerhetspolisens nya lag. I vilken utsträckning loggning bör göras kan regleras i förordning.

I brottsdatalagen begränsas kravet på loggning till behandling i automatiserade behandlingssystem. Skälet för det är att dataskyddsdirektivet föreskriver denna begränsning (prop. 207/18:232 s. 181 f.). Trots *Datainspektionen* avstyrkande i denna del föreligger inte skäl att i den nya lagen avvika från den begränsning som gjorts i brottsdatalagen gällande loggar. Säkerhetspolisens skyldighet att föra loggar bör alltså gälla behandling i automatiserade behandlingssystem.

Med automatiserade behandlingssystem avses för verksamheten särskilt utformade eller anpassade behandlingssystem där personuppgifter behandlas mer eller mindre strukturerat, t.ex. verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. Däremot bör standardprogram som Word, Outlook och Excel, av samma skäl som anges när det gäller dataskydd som standard, inte omfattas av kraven på loggning. Olika lagringsytor, som t.ex. usb-minnen och anställdas personliga mappar på den egna datorn, bör också undantas från de kraven. Personuppgiftsregleringen i övrigt gäller däremot för behandling som utförs i sådan programvara och på sådana lagringsytor även om de inte omfattas av de preciserade kraven på loggning. De närmare detaljerna kan regleras på lägre normgivningsnivå (jfr prop. 2017/18:232 s. 177).

Förslaget att de mer preciserade kraven på loggning ska begränsas till automatiserade behandlingssystem ska inte uppfattas som att kraven på annan behandling av personuppgifter i sådana system är lägre än vad som gäller för behandling i andra system.

Loggning är ett viktigt inslag i det övergripande kravet på att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna, vilket innebär att loggning kan krävas även i andra fall. Vilka uppgifter som kan behöva loggas kan dock variera. Det kan t.ex. vara viktigare med loggning i system som ett flertal personer använder än i system som enbart ett fåtal har tillgång till.

Även om lagens krav på loggning inte gäller i andra system än automatiserade behandlingssystem bör Säkerhetspolisen när det är tekniskt möjligt ha loggning även i sådana system som inte omfattas av kravet. Loggning krävs normalt även där för att ge tillräckligt underlag för intern

kontroll. Dessutom måste Säkerhetspolisen se till att behandling av integritetskänsliga personuppgifter inte utförs vid sidan av automatiserade behandlingssystem i syfte att kringgå lagens krav. Tillsynsmyndigheten bör också i enskilda fall kunna ställa krav på loggning om det är en skydds- eller säkerhetsåtgärd som är nödvändig för att behandlingen ska omgärdas med tillräckligt skydd.

Vad ska loggas?

Enligt förarbetena till brottsdatalagen är utgångspunkten att loggar bör föras över de typer av behandlingar som anges i artikel 25.1 i dataskyddsdirektivet, dvs. insamling, ändring, läsning, utlämning (inklusive överföringar), sammanförande och radering. Därutöver bör även överföringar till tredjeland eller internationella organisationer loggas (prop. 2017/18:232 s. 176–178). Motsvarande bör gälla för Säkerhetspolisen. Det kan dock regleras i förordning eller i föreskrifter på lägre normgivningsnivå.

En behandlingshistorik bör normalt vara utformad så att den avslöjar felaktig eller obehörig användning av personuppgifter. När det gäller läsning och utlämning av personuppgifter ska loggarna göra det möjligt att få fram viss typ av information. Eftersom loggning är ett automatiskt förfarande kan endast viss information om behandlingen dokumenteras. Det rör sig främst om datum och tidpunkt för behandlingen. Information om vem som har behandlat personuppgiften går också att få fram om de anställda har tilldelats behörigheter och det krävs inloggning i systemen. När det gäller utlämnande av uppgifter kan identiteten på den som har lämnat ut uppgifterna endast fastställas om de lämnats ut elektroniskt via systemet. Detsamma gäller överföringar till tredjeland eller internationella organisationer. Det bör dock vara möjligt att logga om en medarbetare har överfört, laddat ner eller skrivit ut uppgifter. Det är däremot inte möjligt att logga om uppgifterna sedan lämnas ut på annat sätt än elektroniskt, t.ex. muntligen eller på papper. Det kan också vara svårt att logga om uppgifterna lämnas ut via e-post.

Hur ska loggarna användas?

Säkerhetspolisen för redan i dag loggar för att uppfylla kraven i 31 § personuppgiftslagen. Tanken är inte att myndigheten ska åläggas att föra ytterligare en logg enbart för personuppgiftsbehandlingen. De system för loggning som i dag används främst i informationssäkerhetssyfte bör normalt kunna användas även för kontroll ur ett integritetsskyddsperspektiv.

Syftet med loggning är att åtkomsten till personuppgifterna ska kunna kontrolleras, bl.a. för att göra det möjligt att utreda felaktig eller obehörig användning av uppgifterna. För att det ska kunna göras måste loggarna sparas en viss tid. Loggning kan också ha en förebyggande funktion. Det förutsätter att användarna informeras om att det förs loggar och att de kontrolleras. Loggningen bör alltså följas upp och loggarna skyddas mot otillåtna ändringar.

Det är viktigt att skilja mellan själva loggningen och uppföljning av loggningen. Logguppföljning bör göras systematiskt och återkommande i syfte att upptäcka och motverka obehörig åtkomst. Uppföljning bör också

göras vid misstanke om att någon obehörigen tagit del av personuppgifter. Det kan vidare finnas anledning att följa upp behandlingshistoriken t.ex. på områden där det finns särskilt integritetskänsliga personuppgifter eller behörigheter som ger stora möjligheter till åtkomst. Det kan också finnas skäl att kontrollera vissa inloggningsmönster. Säkerhetspolisen bör ha rutiner för logguppföljningen. Myndigheten bör exempelvis ge riktlinjer och vägledning till den som kontrollerar loggarna beträffande vad som kan vara obehörig åtkomst. Vid logguppföljning måste också reglerna om meddelarfrihet och efterforskningsförbud i tryckfrihetsförordningen och yttrandefrihetsgrundlagen beaktas, vilket innebär att möjligheten till uppföljning i vissa fall begränsas eller kan vara otillåten.

Det är av största vikt att loggningssystem inte missbrukas eller används för andra syften än som varit avsett. I förarbetena till brottsdatalagen anges att det inte bör författningsregleras hur loggarna får användas, eftersom det skulle riskera att låsa fast myndigheterna vid ett visst arbetssätt eller omöjliggöra användning som kan visa sig vara nödvändig. Det innebär dock inte att användningen av loggar bör vara helt oreglerad. Utöver myndigheternas interna föreskrifter och riktlinjer får tillsynsmyndigheten ge vägledning för användningen av loggar, t.ex. genom allmänna råd och riktlinjer (prop. 2017/18:232 s. 180). Motsvarande bör gälla även för Säkerhetspolisen.

Loggarna utgör sådan dokumentation som tillsynsmyndigheten har rätt att på begäran få del av (avsnitt 15.5). Någon särskild bestämmelse som föreskriver att loggarna ska göras tillgängliga för tillsynsmyndigheten behövs därför inte.

13.2.4 Tillgången till personuppgifter ska begränsas

Regeringens förslag: Säkerhetspolisen ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Av 2 kap. 11 § polisdatalagen framgår att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen gäller för Säkerhetspolisen genom en hänvisning i 6 kap. 4 § 5 polisdatalagen. En motsvarande bestämmelse finns i 3 kap. 6 § brottsdatalagen.

När stora informationsmängder är samlade på ett sådant sätt att integritetskänsliga personuppgifter är enkelt sökbara på elektronisk väg finns det uppenbara risker för intrång i den personliga integriteten. I förarbetena till polisdatalagen påtalas vikten av att det säkerställs att integritetskänsliga personuppgifter görs tillgängliga bara för dem som behöver uppgifterna för sitt arbete. Vem som har rätt att använda personuppgifterna och hur uppgifterna sprids är omständigheter som påverkar risken för intrång i den personliga integriteten (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 94). I förarbetena till den nu upphävda åklagardatalagen konstateras att det är en hörnsten i

skyddet av enskildas integritet att åtkomst endast medges till de personuppgifter som den enskilde tjänstemannen behöver för att kunna utföra sina arbetsuppgifter (prop. 2014/15:63 s. 59).

Ju fler personer i en myndighet som har tillgång till personuppgifter, desto större är risken för obehörig åtkomst eller spridning av uppgifterna. Att utbilda användarna i informationssäkerhets- och dataskyddsfrågor är en viktig organisatorisk säkerhetsåtgärd, men det är ofta inte tillräckligt. Att tillgången till personuppgifter i så stor utsträckning som möjligt faktiskt begränsas till vad var och en behöver för att utföra sitt arbete är viktigt för att skapa ett tillfredsställande internt skydd för personuppgifter vid myndigheters informationshantering.

Mot den bakgrunden finns det ett generellt behov av att begränsa tillgången till personuppgifter. En bestämmelse som motsvarar 3 kap. 6 § brottsdatalagen bör därför tas in i den nya lagen. Säkerhetspolisen ska alltid vara skyldig att pröva anställdas behov av tillgång till personuppgifter utifrån vad arbetsuppgifterna kräver och begränsa tillgången i enlighet med det. Bestämmelsen bör gälla personuppgifter både i Säkerhetspolisens egna system och i system som myndigheten får tillgång till genom direktåtkomst eller andra former av informationsutbyte.

Eftersom bestämmelsen bör vara generell kan det finnas behov av närmare riktlinjer för hur tillgången till personuppgifter bör avgränsas för de enskilda tjänstemännen. Det kan regleras i föreskrifter på myndighetsnivå eller i interna styrdokument hos myndigheten.

13.2.5 Konsekvensbedömning och förhandssamråd med tillsynsmyndigheten

Regeringens förslag: Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser, med hänvisning till uttalanden på dataskyddsförordningens område från den s.k. artikel 29-gruppen, att den personuppgiftsansvarige inte bör vara skyldig att samråda med tillsynsmyndigheten om åtgärder har vidtagits för att minska risken för intrång i den registrerades personliga integritet i tillräcklig omfattning. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Regleringen i brottsdatalagen

Enligt 3 kap. 7 § första stycket brottsdatalagen är den personuppgiftsansvarige skyldig att göra konsekvensbedömningar. En konsekvensbedömning ska göras om det kan antas att en ny typ av behandling kommer att medföra särskild risk för intrång i registrerades personliga integritet. Detsamma gäller om betydande förändringar av redan pågående behandlingar förväntas leda till sådan risk. Vid riskbedömningen ska bl.a. användningen av ny teknik och behandlingens art, omfattning, sammanhang och ändamål beaktas. En konsekvensbedömning ska omfatta relevanta system och processer för behandlingen, men inte behandlingen i enskilda fall (se prop. 2017/18:232 s. 181 f.).

I 3 kap. 7 § andra stycket regleras förhandssamråd. När en konsekvensbedömning visar att det finns särskild risk för intrång i registrerades personliga integritet ska den personuppgiftsansvarige samråda med tillsynsmyndigheten. Samråd aktualiseras också om typen av behandling, särskilt med beaktande av ny teknik, nya rutiner eller nya förfaranden, i sig innebär särskild risk för intrång i registrerades personliga integritet och en konsekvensbedömning med anledning av det har gjorts. I sådana fall är resultatet av konsekvensbedömningen inte avgörande för om samråd med tillsynsmyndigheten ska äga rum. För att underlätta för den personuppgiftsansvarige och för att säkerställa att förhandssamrådet träffar rätt situationer kan tillsynsmyndigheten genom föreskrifter ange vilka typer av behandlingar som ska omfattas av förhandssamråd.

Säkerhetspolisen bör göra konsekvensbedömningar och genomföra förhandssamråd

I 2 § polisdataförordningen (2010:1155) regleras när Säkerhetspolisen ska samråda med Datainspektionen. Sådant samråd ska äga rum när myndigheten planerar nya it-system av större omfattning eller nya it-system som kan innebära särskilda risker för intrång i den personliga integriteten och när det genomförs betydande förändringar i sådana system. Samråd ska äga rum i god tid innan beslut i frågan fattas. Paragrafen föreskriver även samråd med Säkerhets- och integritetsskyddsnämnden i vissa frågor. Polismyndigheten hade tidigare motsvarande samrådsskyldighet och Kustbevakningen skulle i liknande situationer samråda med Datainspektionen.

För Polismyndigheten och Kustbevakningen har samrådsskyldigheten ersatts av regleringen i 3 kap. 7 § brottsdatalagen. För att uppnå enhetlighet för tillsynsmyndigheten bör enligt regeringens mening samrådsskyldigheten för Säkerhetspolisen formuleras på samma sätt som i brottsdatalagen. Regeringen återkommer till frågan om vilken tillsynsmyndighet som Säkerhetspolisen ska samråda med i avsnitt 15.

Det är viktigt att samrådet äger rum så tidigt i utvecklingsprocessen som möjligt. Då kan frågor om integritetsskydd beaktas på ett bättre sätt. Samtidigt bör förhandssamrådet inte äga rum så tidigt att det inte finns något konkret förslag på teknisk lösning för tillsynsmyndigheten att ta ställning till. Samrådet bör äga rum i god tid innan behandlingen påbörjas eller större förändringar av redan pågående behandlingar genomförs.

Datainspektionen anser att samråd inte ska behöva hållas när den personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att minska risken för intrång. Som anges i förarbetena till brottsdatalagen kan det vara svårt för den personuppgiftsansvarige att på egen hand avgöra vilka åtgärder som är tillräckliga. Det är dock inte uteslutet att vidtagna åtgärder från den personuppgiftsansvariges sida kan befria från samrådsskyldigheten. Regeringen har i förarbetena till brottsdatalagen bedömt att frågan om i vilken utsträckning samråd inte borde krävas för att den personuppgiftsansvarige har vidtagit åtgärder som minskat risken för intrång till en godtagbar nivå får överlämnas åt rättstillämpningen (prop. 2017/18:232 s. 188). Det finns inte skäl att nu göra någon annan bedömning.

Eftersom samrådsskyldigheten i brottsdatalagen är knuten till skyldigheten att göra konsekvensbedömningar bör även Säkerhetspolisen ha motsvarande skyldighet att göra konsekvensbedömningar som behöriga myndigheter har enligt brottsdatalagen. Säkerhetspolisens skyldighet att samråda med tillsynsmyndigheten kommer härigenom att förändras något, men regeringen anser i likhet med utredningen att kravet på konsekvensbedömning fyller en viktig funktion ur ett integritetsperspektiv. Det bör regleras vilken information konsekvensbedömningen ska innehålla och att den ska dokumenteras, men detta kan göras i förordning.

Vid förhandssamråd bör Säkerhetspolisen lämna in konsekvensbedömningen och eventuell annan information som tillsynsmyndigheten kan behöva för sin prövning.

Tillsynsmyndighetens befogenheter

Tillsynsmyndigheten ska inom ramen för förhandssamrådet använda sina befogenheter, om den anser att den planerade behandlingen inte kommer att vara författningsenlig. Tillsynsmyndigheten bör i dessa situationer ha möjlighet att använda sina förebyggande befogenheter gentemot Säkerhetspolisen. Tillsynsmyndigheten ska inom ramen för förhandssamrådet ge Säkerhetspolisen skriftliga råd. Tillsynsmyndigheten har också möjlighet att utfärda varning för att behandla personuppgifterna på det planerade sättet (avsnitt 15.5.3). Om Säkerhetspolisen ignorerar råden och varningen och påbörjar behandlingen kan tillsynsmyndigheten vidta andra åtgärder, t.ex. utfärda ett föreläggande (avsnitt 15.5.4). Korrigerande åtgärder ska dock inte vidtas inom ramen för förhandssamrådet utan är i stället ett led i tillsynsmyndighetens allmänna tillsynsuppgifter enligt lagen.

Detaljbestämmelser om tillsynsmyndighetens roll vid förhandssamråd motsvarande dem som finns i brottsdataförordningen (2018:1202) kan även för Säkerhetspolisens del finnas i förordning.

13.2.6 Samarbete med tillsynsmyndigheten

Regeringens förslag: Säkerhetspolisen ska samarbeta med tillsynsmyndigheten när den utför sina uppgifter enligt lagen och föreskrifter som har meddelats i anslutning till lagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna har inte något att invända mot förslaget.

Skälen för regeringens förslag: I 3 kap. 12 § brottsdatalagen föreskrivs att den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den. Någon sådan uttrycklig skyldighet har inte funnits tidigare. Samarbetsskyldigheten innebär inte bara att den personuppgiftsansvarige ska ge tillsynsmyndigheten tillgång till det material och de resurser som den har rätt till. Bestämmelsen innebär även att den personuppgiftsansvarige ska underlätta för tillsynsmyndigheten att utöva sina tillsynsbefogenheter på ett effektivt sätt. Även om tillsynsmyndigheten inte får använda tvång mot den personuppgiftsansvarige för att kunna utöva sin tillsyn är det viktigt att den personuppgiftsansvarige ges en uttrycklig skyldighet att samarbeta med tillsynsmyndigheten (prop. 2017/18:232 s. 189 f.). Samarbetsskyldigheten aktualiseras när tillsynsmyndigheten utför sina uppgifter enligt brottsdatalagen och de föreskrifter som utfärdas i anslutning till den. Den personuppgiftsansvarige är således skyldig att samarbeta med tillsynsmyndigheten när den bl.a. utövar allmän tillsyn över personuppgiftsbehandling.

Det är rimligt att kräva att Säkerhetspolisen i samma utsträckning som andra brottsbekämpande myndigheter ska samarbeta med den myndighet som enligt lagen utövar tillsyn över myndighetens personuppgiftsbehandling. En bestämmelse motsvarande 3 kap. 12 § brottsdatalagen om skyldigheten att samarbeta med tillsynsmyndigheten bör därför tas in i den nya lagen.

Vad samarbetsskyldigheten mer konkret kommer att innebära för Säkerhetspolisen hör samman med vilka befogenheter som tillsynsmyndigheten ges. Den frågan behandlas i avsnitt 15.

13.2.7 Säkerheten för personuppgifter

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

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser att de faktorer som anges i artikel 29.1 i dataskyddsdirektivet bör komma till uttryck i lagen i stället för i förordning. Övriga remissinstanser yttrat sig inte särskilt i denna del.

Skälen för regeringens förslag

I 31 § första stycket personuppgiftslagen föreskrivs att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas och att åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur känsliga de behandlade personuppgifterna är. Vidare föreskrivs i 32 § personuppgiftslagen att tillsynsmyndigheten i enskilda fall får besluta om säkerhetsåtgärder enligt 31 §. Bestämmelserna gäller för Säkerhetspolisen

genom hänvisningar i 2 kap. 2 § första stycket 7 och 6 kap. 4 § 1 polisdatalagen. Bestämmelser om informationssäkerhet finns även i andra författningar, t.ex. i arkivlagen (1990:782) och säkerhetsskyddslagen (2018:585) med tillhörande förordningar och föreskrifter samt i föreskrifter meddelade av Myndigheten för samhällsskydd och beredskap (exempelvis MSBFS 2016:1 Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet).

I 3 kap. 8 § brottsdatalagen regleras vilka skyddsåtgärder den personuppgiftsansvarige ska vidta. Regleringen motsvarar 31 § personuppgiftslagen och gäller således för Säkerhetspolisen i dag. En bestämmelse med motsvarande innehåll bör tas in i den nya lagen. I brottsdatalagen har skyldigheten preciserats genom att det anges att personuppgifterna särskilt ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom oavsiktliga händelser. Motsvarande precisering bör göras i den nya lagen.

Regeringen anser i likhet med utredningen, men till skillnad från *Datainspektionen*, att vilka omständigheter som bör beaktas för att uppnå en lämplig skyddsnivå kan regleras i förordning. Utöver de omständigheter som anges i 31 § personuppgiftslagen bör behandlingens art, omfattning, sammanhang och ändamål beaktas. Särskild hänsyn bör tas till i vilken utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är. (jfr prop. 2017/18:232 s. 196).

13.2.8 Ingen skyldighet att anmäla personuppgiftsincidenter

Regeringens bedömning: Säkerhetspolisen bör inte vara skyldig att anmäla personuppgiftsincidenter till tillsynsmyndigheten.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Försvarets radioanstalt* instämmer i utredningens bedömning. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning: I 3 kap. 9–11 §§ brottsdatalagen regleras den personuppgiftsansvariges skyldigheter vid en personuppgiftsincident. Där föreskrivs bl.a. att sådana incidenter ska anmälas till tillsynsmyndigheten inom viss tid och att den registrerade i vissa fall ska underrättas om incidenten. Enligt 3 kap. 9 § första stycket gäller anmälningsskyldigheten inte om personuppgiftsincidenten rör nationell säkerhet.

It-incidenter ska som huvudregel anmälas till Myndigheten för samhällsskydd och beredskap. Det framgår av 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Det gäller dock inte sådana it-incidenter som enligt 2 kap. 10 § första stycket 2 säkerhetsskyddsförordningen (2018:658) ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Exempel på sådana incidenter är incidenter i informationssystem där uppgifter som gäller Sveriges säkerhet behandlas. Behovet av att skydda sådan information anses vara så stort att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Mot bakgrund av det,

och då nationell säkerhet ligger utanför direktivets tillämpningsområde, har personuppgiftsincidenter som rör nationell säkerhet undantagits från anmälningsskyldigheten i brottsdatalagen. Motsvarande undantag gäller enligt 1 kap. 4 § dataskyddslagen.

Den nya lagen ska tillämpas vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Personuppgiftsincidenter som inträffar i myndighetens informationssystem och som drabbar personuppgifter som behandlas med stöd av den nya lagen kommer alltid att röra nationell säkerhet och därmed, enligt brottsdatalagens reglering, vara undantagna från anmälningsskyldighet. Det finns därför inte skäl att i den nya lagen ta in bestämmelser som reglerar anmälan av personuppgiftsincidenter till tillsynsmyndigheten.

13.3 Dataskyddsombud

13.3.1 Definition av dataskyddsombud

Regeringens förslag: Dataskyddsombud ska i lagen definieras som den fysiska person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Datainspektionen* anser att definitionen av dataskyddsombud bör inkludera juridiska personer. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 3 § personuppgiftslagen definieras personuppgiftsombud, som motsvarar det som i dataskyddsdirektivet kallas dataskyddsombud. Där anges att ett personuppgiftsombud är den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Personuppgiftsombud är visserligen ett inarbetat begrepp, men dataskyddsombud är den term som används både i brottsdatalagen och i dataskyddsförordningen. Den termen bör därför användas även i den nya lagen.

Dataskyddsombud bör definieras i lagen. Eftersom dataskyddsombudet föreslås vara en anställd hos Säkerhetspolisen (avsnitt 13.3.2) kan definitionen inte, till skillnad från vad *Datainspektionen* anfört, inkludera juridiska personer. Det bör i stället framgå av definitionen att dataskyddsombudet ska vara en fysisk person. I övrigt bör definitionen överensstämma med motsvarande definition i brottsdatalagen. Dataskyddsombud är således den fysiska person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

13.3.2 Krav att utse dataskyddsombud

Regeringens förslag: Säkerhetspolisen ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* välkomnar förslaget att Säkerhetspolisen ska vara skyldig att utse dataskyddsombud. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 3 kap. 13 § brottsdatalagen ska den personuppgiftsansvarige utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas. Säkerhetspolisen har i dag enligt 6 kap. 5 § andra stycket polisdatalagen en skyldighet att utse personuppgiftsombud och bör liksom övriga brottsbekämpande myndigheter även fortsättningsvis vara skyldig att utse ett eller flera dataskyddsombud. En bestämmelse om skyldighet att utse dataskyddsombud bör därför tas in i den nya lagen.

Dataskyddsombud bör vara en anställd hos Säkerhetspolisen. Kraven på dataskyddsombudets kvalifikationer kan anges i förordning.

Säkerhetspolisen bör anmäla till tillsynsmyndigheten vem som har utsetts till dataskyddsombud och när ombudet entledigas. Det är viktigt att tillsynsmyndigheten får information om det, eftersom ombuden bl.a. ska ha till uppgift att samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den i vissa fall (avsnitt 13.3.3).

13.3.3 Dataskyddsombudens arbetsuppgifter

Regeringens förslag: Dataskyddsombud ska ha vissa i lagen angivna arbetsuppgifter.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska dataskyddsombud vara skyldiga att anmäla till tillsynsmyndigheten om Säkerhetspolisen bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering

Enligt 38–40 §§ personuppgiftslagen ska personuppgiftsombud självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed och påpeka eventuella brister. Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter, och vidtas inte rättelse efter påpekande, ska ombudet anmäla det till tillsynsmyndigheten. Personuppgiftsombud ska även i övrigt samråda med tillsynsmyndigheten. Personuppgiftsombuden ska också föra förteckning över de behandlingar som den personuppgiftsansvarige utför och som skulle ha omfattats av anmälningsskyldighet om inte ombudet hade funnits. Personuppgiftsombud ska

dessutom hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Dessa bestämmelser gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 9 och 6 kap. 4 § 1 polisdatalagen.

Ombudens arbetsuppgifter bör vara desamma som enligt brottsdatalagen

Dataskyddsombudens roll påminner i stora delar om personuppgiftsombudens. Dataskyddsombuden har dock genom brottsdatalagen fått delvis nya arbetsuppgifter och en något förändrad roll. Flertalet av de arbetsuppgifter som ska anförtros dataskyddsombud har t.ex. karaktären av intern rådgivning, vilket inte är fallet i dag. Dataskyddsombuden har också fått ett tydligare uppdrag att bistå tillsynsmyndigheten. Eftersom dataskyddsombudens arbetsuppgifter bör vara enhetliga bör bestämmelser motsvarande 3 kap. 14 § brottsdatalagen tas in i den nya lagen. Säkerhetspolisens dataskyddsombud kommer därmed att få en något förändrad roll och några fler arbetsuppgifter.

I den nya lagen bör det således föreskrivas att dataskyddsombud självständigt ska kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör de skyldigheter som åligger myndigheten som personuppgiftsansvarig. Självständighetskravet innebär att Säkerhetspolisen inte bör utse ett ombud som har en alltför underordnad ställning i organisationen. För att ombudet ska vara oberoende måste han eller hon också ha tillräckliga kvalifikationer och kunskaper för att kunna utföra sina arbetsuppgifter på ett självständigt sätt.

Dataskyddsombud bör vidare informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter enligt lagen och andra författningar som rör personuppgiftsbehandling. Det handlar främst om att göra Säkerhetspolisen och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att informera registrerade, att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Om Säkerhetspolisen begär det ska ombudet ge råd vid en konsekvensbedömning och kontrollera att bedömningen genomförs på rätt sätt.

Dataskyddsombudens roll påminner i dessa delar om internrevisorers. För att ombuden ska kunna utöva intern kontroll bör de inte ges arbetsuppgifter som kan komma i konflikt med kontrolluppgiften. Det kan t.ex. vara olämpligt att låta dataskyddsombud utbilda personalen eller ansvara för att den får annan information, eftersom det är åtgärder som omfattas av den interna granskningen. Det är viktigt att dataskyddsombudet trots sin dubbla roll kan utöva kontrollen på ett oberoende sätt.

Enligt personuppgiftslagen ska ett personuppgiftsombud anmäla till tillsynsmyndigheten om han eller hon misstänker att den personuppgiftsansvarige bryter mot gällande bestämmelser och inte vidtar rättelse. Som utredningen påpekar är det viktigt att dataskyddsombud uppmärksammar tillsynsmyndigheten på eventuella problem och brister, särskilt om den personuppgiftsansvarige inte rättar sig efter ombudets påpekanden. Med hänsyn till att motsvarande anmälningsskyldighet inte gäller på dataskyddsförordningens område var det enligt regeringen inte motiverat att införa en sådan skyldighet i brottsdatalagen (prop. 2017/18:232 s. 210).

Någon sådan anmälningsskyldighet bör därför inte heller införas i den nya lagen.

Dataskyddsombud bör även samarbeta med och fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter. Det gäller särskilt vid sådant förhandssamråd som avses i avsnitt 13.2.5. Samarbetet innebär också att ombudet, när det är lämpligt, ska samråda med tillsynsmyndigheten även i andra frågor som rör personuppgiftsbehandling.

Dataskyddsombud bör också ha samma roll i förhållande till enskilda som personuppgiftsombud har i dag. De bör därför vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter.

Dataskyddsombudens verksamhet ska underlättas

För att dataskyddsombuden ska kunna utföra sina arbetsuppgifter krävs det att Säkerhetspolisen gör det möjligt och tillhandahåller de resurser som ombuden behöver, genom att t.ex. göra ombudet delaktig i frågor och beslut som rör behandling av personuppgifter. Ombuden bör också få tillgång till all dokumentation gällande personuppgiftsbehandlingen och, i den utsträckning det behövs, tillgång till de personuppgifter som behandlas. Säkerhetspolisen bör även se till att ombudet ges utrymme för vidareutbildning och annan kunskapsinhämtning. Bestämmelser om detta kan tas in i förordning.

13.4 Personuppgiftsbiträden

13.4.1 Definition av personuppgiftsbiträde

Regeringens förslag: Personuppgiftsbiträde ska i lagen definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

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

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 1 kap. 6 § brottsdatalagen definieras personuppgiftsbiträde som den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Definitionen motsvarar 3 § personuppgiftslagen. Utredningen anser att det ska framgå av definitionen att det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse mellan personuppgiftsbiträdet och den personuppgiftsansvarige. I förarbetena till brottsdatalagen konstateras att dataskyddsdirektivet inte ställer något sådant krav och regeringen valde därför att inte låta brottsdatalagens definition innehålla något sådant krav (prop. 2017/18:232 s. 206). För att underlätta tillämpningen bör definitionen av personuppgiftsbiträde i den nya lagen stämma överens med brottsdatalagens definition. Personuppgiftsbiträde bör mot den bakgrunden definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Därmed kommer definitionen också att överensstämma med den som finns i dataskyddsförordningen.

Ett personuppgiftsbiträde måste alltid finnas utanför den personuppgiftsansvariges organisation. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

13.4.2 Anlitande av personuppgiftsbiträden

Regeringens förslag: Säkerhetspolisen ska, om det är lämpligt, få anlita personuppgiftsbiträden. Innan ett personuppgiftsbiträde anlitas ska Säkerhetspolisen försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbiträdets behandling av personuppgifter för Säkerhetspolisens räkning.

Ett personuppgiftsbiträde ska inte få anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från Säkerhetspolisen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Umeå universitet* och *Sveriges advokatsamfund* efterfrågar en analys av hur reglerna om möjligheten för Säkerhetspolisen att anlita personuppgiftsbiträden förhåller sig till olika sekretessbestämmelser och säkerhetskrav. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering

Regler om personuppgiftsbiträden finns i 30 och 31 §§ personuppgiftslagen. Bestämmelserna gäller för Säkerhetspolisen genom en hänvisning i 2 kap. 2 § första stycket 7 och 6 kap. 4 § 1 polisdatalagen. Enligt 31 § andra stycket ska den personuppgiftsansvarige, när denne anlitar ett personuppgiftsbiträde, förvissa sig om att biträdet kan vidta de säkerhetsåtgärder som krävs och se till att biträdet gör det. Det är dock den personuppgiftsansvarige som har ansvaret gentemot den registrerade även när ett personuppgiftsbiträde anlitas (Personuppgiftslagen, prop. 1997/98:44, s. 93). Det ska enligt 30 § andra stycket personuppgiftslagen finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet ska vidta de säkerhetsåtgärder som avses i 31 § första stycket för att skydda personuppgifterna.

Personuppgiftsbiträden ska kunna anlitas

I 3 kap. 16 § brottsdatalagen föreskrivs att den personuppgiftsansvarige, om det är lämpligt, får anlita personuppgiftsbiträden för behandling av personuppgifter på den personuppgiftsansvariges vägnar.

Säkerhetspolisen får i dag anlita personuppgiftsbiträden. Utrymmet att anlita personuppgiftsbiträden är dock begränsat med hänsyn till den verksamhet som myndigheten bedriver. Myndigheten bör dock även fortsättningsvis ha möjlighet att anlita personuppgiftsbiträden om det är lämpligt och en bestämmelse som motsvarar 3 kap. 16 § brottsdatalagen bör därför tas in i den nya lagen. Om det är lämplig får avgöras med hänsyn bl.a. till vilka personuppgifter som ska behandlas och om det gäller sekretess för personuppgifterna. Någon mer djuplodande analys av sekretessbestämmelsernas betydelse för Säkerhetspolisens möjlighet att anlita personuppgiftsbiträden, som *Umeå universitet* och *Sveriges advokatsamfund* efterfrågar, är mot den bakgrunden inte nödvändig.

Säkerhetspolisen bör innan ett personuppgiftsbiträde anlitas försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter. Skyldigheten innebär att myndigheten innan ett personuppgiftsbiträde anlitas bl.a. bör förhöra sig om hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna har hos biträdet. Bestämmelsen går något längre än de nu gällande kraven på personuppgiftsansvariga.

Ansvarsfördelningen mellan den personuppgiftsansvarige och personuppgiftsbiträdet

Säkerhetspolisen är ansvarig för all behandling av personuppgifter som utförs på dennes vägnar. Myndigheten ansvarar således både i förhållande till tillsynsmyndigheten och i förhållande till registrerade för att reglerna i lagen och andra tillämpliga författningar följs vid personuppgiftsbehandling hos ett personuppgiftsbiträde. Säkerhetspolisen kan uppdra åt biträdet att utföra viss behandling av personuppgifter, men kan inte avsäga sig personuppgiftsansvaret och de skyldigheter som följer med det. Myndigheten är också skadeståndsskyldig gentemot enskilda vid felaktig behandling av personuppgifter hos personuppgiftsbiträdet. Att biträdet kan bli skadeståndsskyldigt gentemot den personuppgiftsansvarige är en annan sak.

Tillsynsmyndigheten får i vissa fall utkräva ansvar även av personuppgiftsbiträden. Om ett personuppgiftsbiträde t.ex. inte vidtar nödvändiga säkerhetsåtgärder kan tillsynsmyndigheten vidta åtgärder mot både biträdet och den personuppgiftsansvarige.

Personuppgiftsbiträdets roll ska regleras i en överenskommelse

På samma sätt som i dag bör det krävas ett skriftligt avtal eller någon annan skriftlig överenskommelse mellan personuppgiftsbiträdet och Säkerhetspolisen. Regleringen av vad ett sådant avtal ska innehålla bör motsvara de krav som ställs på dessa avtal enligt 3 kap. 17 § brottsdataförordningen. Även för Säkerhetspolisens del kan det regleras i förordning.

Anlitande av underbiträden

Personuppgiftslagen reglerar inte förutsättningarna för när ett personuppgiftsbiträde får anlita ett annat personuppgiftsbiträde, ett underbiträde.

Det är av grundläggande betydelse att den personuppgiftsansvarige känner till vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning. I 3 kap. 17 § brottsdatalagen föreskrivs det därför att ett personuppgiftsbiträde inte får anlita ett annat personuppgiftsbiträde utan att den personuppgiftsansvarige har lämnat skriftligt tillstånd till det. En motsvarande bestämmelse bör tas in i den nya lagen. Att personuppgiftsbiträden som har fått ett generellt tillstånd att anlita underbiträden ska vara skyldiga att informera Säkerhetspolisen när underbiträden anlitas kan regleras i förordning. Syftet med informationen är att Säkerhetspolisen ska ha möjlighet att invända mot anlitandet av nya biträden.

13.4.3 Behandling enligt den personuppgiftsansvariges instruktioner

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

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

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: I 30 § första stycket personuppgiftslagen, som gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 7 och 6 kap. 4 § 1 polisdatalagen, föreskrivs att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det allmännas verksamhet i sådana frågor, gäller emellertid de bestämmelserna i stället för 30 § första stycket. Det som främst avses är bestämmelser om tystnadsplikt och sekretess (prop. 1997/98:44 s. 134). En motsvarande bestämmelse finns i artikel 23 dataskyddsdirektivet som har genomförts i 3 kap. 18 § första stycket brottsdatalagen. Även i den nya lagen bör det tas in en bestämmelse av vilken det framgår att ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen.

Instruktionerna bör vara så tydliga att otillåten behandling inte utförs (jfr Integritet, Offentlighet, Informationsteknik, SOU 1997:39 s. 335). Den överenskommelse som styr personuppgiftsbiträdets uppdrag ska innehålla viss information som ger instruktioner till biträdet, bl.a. om behandlingens varaktighet, art och ändamål. Instruktionerna kan också gälla exempelvis hur tillgången till personuppgifter hos biträdet ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för dataskydd. Ett personuppgiftsbiträde bör endast överföra

personuppgifter till ett tredjeland eller en internationell organisation om biträdet fått i uppdrag att göra det. Sådana uppdrag bör också framgå av de instruktioner som den personuppgiftsansvarige lämnar till biträdet.

Eftersom den nya lagen är subsidiär kommer avvikande bestämmelser i annan författning att gälla framför bestämmelser i den nya lagen, vilket framgår av den föreslagna bestämmelsen i 1 kap. 4 §. Om det finns avvikande bestämmelser i annan författning som anger att någon är skyldig att utföra en viss behandling, exempelvis att lämna ut allmänna handlingar, innebär det att behandlingen får utföras utan särskilda instruktioner.

Att den som bestämmer ändamålen med och medlen för behandlingen är att anse som personuppgiftsansvarig framgår av definitionen av personuppgiftsansvarig. På samma sätt som i brottsdatalagen bör det i den nya lagen tydliggöras att ett personuppgiftsbiträde som går utanför sin befogenhet och behandlar personuppgifter för något annat ändamål än enligt sina instruktioner är personuppgiftsansvarig för den behandlingen. I sådana fall kan biträdet bli skadeståndsskyldig på grund av den behandlingen.

13.4.4 Övriga skyldigheter för personuppgiftsbiträden

Regeringens förslag: Ett personuppgiftsbiträde ska ha samma skyldigheter som en personuppgiftsansvarig att logga vissa typer av behandlingar, begränsa tillgången till personuppgifter, vidta säkerhetsåtgärder och samarbeta med tillsynsmyndigheten.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Flera av skyldigheterna för personuppgiftsansvariga enligt brottsdatalagen gäller även för personuppgiftsbiträden. Som framgår av 3 kap. 19 § brottsdatalagen gäller bestämmelserna om skyldighet att logga vissa typer av behandlingar, samarbeta med tillsynsmyndigheten och vidta lämpliga åtgärder för att skydda personuppgifterna även för personuppgiftsbiträden. Skyldigheten att begränsa tillgången till personuppgifter till vad var och en behöver för att fullgöra sina arbetsuppgifter gäller även för personuppgiftsbiträden. Förhandssamråd med tillsynsmyndigheten är dock bara en skyldighet för den personuppgiftsansvarige, eftersom denne är ansvarig även för den behandling som personuppgiftsbiträdet utför. Ett personuppgiftsbiträde kan emellertid behöva bistå den personuppgiftsansvarige under förhandssamrådet om samrådet t.ex. rör förändringar avseende redan pågående personuppgiftsbehandling som utförs av biträdet. Skyldigheten att samarbeta med tillsynsmyndigheten gäller även för personuppgiftsbiträden. Samarbetsskyldigheten gäller generellt och omfattar därigenom även samarbete från biträdets sida vid förhandssamråd om det blir aktuellt. En motsvarande reglering bör tas in i den nya lagen.

Regleringen av personuppgiftsbiträdens skyldigheter medför inga större skillnader i förhållande till dagens reglering. Enligt 30 § andra stycket personuppgiftslagen är ett personuppgiftsbiträde skyldigt att vidta sådana säkerhetsåtgärder som avses i 31 § första stycket. Det ska också föreskrivas i biträdesavtalet. Personuppgiftsbiträden är alltså redan i dag

skyldiga att vidta lämpliga åtgärder för att skydda de personuppgifter som behandlas. Det innebär ett indirekt krav på att begränsa tillgången till personuppgifter genom exempelvis behörighetstilldelning och att logga behandlingar för att kunna kontrollera åtkomsten till personuppgifterna. Den enda nyheten är att tillsynsmyndigheten kan vidta åtgärder mot både Säkerhetspolisen och personuppgiftsbiträden om de brister i sina skyldigheter. Eftersom Säkerhetspolisen fortfarande är ansvarig för den behandling som personuppgiftsbiträdet utför torde det sällan bli aktuellt att utnyttja den möjligheten.

14 Enskildas rättigheter

14.1 Tydligare reglering av enskildas rättigheter

14.1.1 Nuvarande reglering

I 23 och 25–27 §§ personuppgiftslagen (1998:204), som genom hänvisningar i 2 kap. 2 § första stycket 5 och 6 kap. 4 § 1 polisdatalagen (2010:361) ska tillämpas av Säkerhetspolisen, regleras vilken information som ska lämnas till den registrerade och när informationsskyldigheten inte gäller. I 23 § personuppgiftslagen regleras vad som gäller om uppgifterna har lämnats av den registrerade själv. För Säkerhetspolisen görs undantag från informationsskyldigheten i 23 § dels vid insamling av personuppgifter genom bilder eller ljud, dels om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen (2 kap. 2 § tredje stycket och 6 kap. 4 § 1 polisdatalagen).

I 25 § första stycket personuppgiftlagen regleras vilken information som Säkerhetspolisen ska lämna självmant. Uppgift om myndighetens identitet ska alltid lämnas och uppgift om ändamålen med behandlingen. All annan information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen ska också lämnas, t.ex. information om mottagarna av uppgifterna, skyldigheten att lämna uppgifter och rätten att ansöka om information och att få rättelse. Enligt 25 § andra stycket behöver information inte lämnas om sådant som den registrerade redan känner till.

Enligt 26 § personuppgiftslagen är Säkerhetspolisen skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller inte. Om sådana uppgifter behandlas ska också skriftlig information lämnas om vilka uppgifter om den sökande som behandlas, varifrån dessa uppgifter har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Av 27 § framgår att undantag från informationsskyldigheten gäller vid sekretess och tystnadsplikt.

I 28 § personuppgiftslagen, som genom hänvisningar i 2 kap. 2 § första stycket 6 och 6 kap. 4 § 1 polisdatalagen gäller för Säkerhetspolisen, regleras Säkerhetspolisens skyldighet att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte har

behandlats på det sätt som föreskrivs i lagen eller föreskrifter som har utfärdats med stöd av den.

14.1.2 Merparten av bestämmelserna om enskildas rättigheter bör tillämpas av Säkerhetspolisen

En del i personuppgiftsskyddet är enskildas rätt att få veta hur deras personuppgifter behandlas. Information om den personuppgiftsbehandling som pågår är en förutsättning för att enskilda ska kunna kontrollera om behandlingen är författningsenlig och i övrigt kunna bevaka sina intressen. Dataskyddsdirektivet medför att rättigheterna för enskilda tydliggörs. Artiklarna om enskildas rättigheter har genomförts i 4 kap. brottsdatalagen (2018:1177). Regeringen instämmer i utredningens bedömning att det i princip bör ställas samma krav på Säkerhetspolisen som på andra myndigheter när det gäller enskildas rättigheter. På så sätt blir det lättare för den enskilde att ta tillvara sina rättigheter. Regleringen i brottsdatalagen skiljer sig inte heller i någon större utsträckning från vad som tidigare gällt enligt personuppgiftslagen. Enligt regeringens bedömning kan merparten av bestämmelserna i 4 kap. brottsdatalagen också tillämpas av Säkerhetspolisen. Mot den bakgrunden bör därför huvuddelen av bestämmelserna i brottsdatalagen som reglerar enskildas rättigheter ha sin motsvarighet i den nya lagen.

14.2 Rätten till information

14.2.1 Allmän information som ska göras tillgänglig

Regeringens förslag: Säkerhetspolisen ska göra viss allmän information tillgänglig för den registrerade. Bland annat ska kategorier av ändamål för behandlingen göras tillgänglig.

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

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 4 kap. 1 § brottsdatalagen anges vilken information den personuppgiftsansvarige på eget initiativ ska göra tillgänglig för den registrerade. Det är information om den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter och kategorier av ändamål för behandlingen. Även information om rätten att begära tillgång till personuppgifter och att begära rättelse, radering och begränsning av behandlingen och möjligheten att lämna in klagomål till en tillsynsmyndighet och dess kontaktuppgifter, ska göras tillgänglig. I kravet på att information ska vara tillgänglig ligger att de registrerade i princip ska ha möjlighet att ta del av informationen när de önskar. Informationen kan t.ex. publiceras på myndighetens webbplats eller finnas i en broschyr, folder eller annan informationsskrift.

Att kategorier av ändamål ska göras tillgänglig innebär att det är fråga om upplysningar av generell karaktär som gäller den behöriga

myndighetens personuppgiftsbehandling i allmänhet. Det innebär att det inte är fråga om ändamålen för behandling i varje enskilt fall som avses utan för vilka kategorier av ändamål personuppgifter får behandlas t.ex. för förundersökningar. Det är tillräckligt att enskilda genom uppräkningen får en god bild av den personuppgiftsbehandling som den behöriga myndigheten utför (Brottsdatalagen, prop. 2017/18:232, s. 232).

I Säkerhetspolisen nya lag bör det finnas en bestämmelse som reglerar myndighetens skyldighet att självmant göra allmän information om myndighetens personuppgiftbehandling tillgänglig. Bestämmelsen bör i huvudsak utformas på samma sätt som i brottsdatalagen. I brottsdatalagen föreskrivs dock att behöriga myndigheter också ska informera om möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifter till den. Det beror på att direktivet kräver det och innehåller en särskild reglering för handläggning av klagomål. Utredningen föreslår ingen motsvarande reglering för Säkerhetspolisen. Ingen remissinstans har heller ansett att det behövs. Säkerhetspolisens informationsskyldighet bör därför inte omfatta sådana uppgifter.

Vilka krav som ska ställas på utformningen av informationen till enskilda kan regleras i förordning.

14.2.2 Information som ska lämnas på begäran

Regeringens förslag: Säkerhetspolisen ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av uppgifterna och få viss skriftlig information om behandlingen.

Sökanden behöver inte få del av personuppgifter som han eller hon redan har tagit del av, om det inte begärs. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 4 kap 3 § första stycket brottsdatalagen ska den personuppgiftsansvarige till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om den personuppgiftsansvarige behandlar personuppgifter om en sökande ska alltså han eller hon få del av uppgifterna när det efterfrågas. Det rör dock endast uppgifter som behandlas vid tiden för utlämnandet.

Utgångspunkten är att sökanden ska få tillgång till all information som den personuppgiftsansvarige själv kan få fram om honom eller henne. Det förutsätter att det finns uppgifter som direkt kan hänföras till den person som begär informationen. Sökanden måste därför lämna sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen. Det kan t.ex. vara fullständigt namn eller person- eller samordningsnummer.

Om personuppgifter som rör sökanden behandlas ska sökanden få del av dem samt få skriftlig information om vilka uppgifter som behandlas och varifrån dessa kommer. Information om varifrån personuppgifterna kommer behöver bara avse den information som finns tillgänglig. Vidare

ska sökanden informeras om de kategorier av personuppgifter som behandlingen gäller. Kategorier av personuppgifter kan t.ex. vara adressuppgifter eller fordonsuppgifter. Även behandlingens rättsliga grund ska framgå. Den personuppgiftsansvarige ska vidare informera om ändamålen med behandlingen. Det som avses är ändamålen med behandlingen i det enskilda fallet.

Information om mottagare eller kategorier av mottagare av personuppgifterna ska också lämnas. Med mottagare avses i brottsdatalagen den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision (avsnitt 7.7). Den personuppgiftsansvarige behöver således inte informera sökanden om att uppgifter har lämnats ut till myndigheter för tillsyn, t.ex. till Justitiekanslern eller Säkerhets- och integritetsskyddsnämnden. Eftersom en myndighet enligt 2 kap. 14 § tryckfrihetsförordningen varken får efterfråga eller dokumentera vilka som tar del av allmänna handlingar med personuppgifter behöver inte heller uppgifter om sådana mottagare lämnas ut (Myndighetsdatalagen, SOU 2015:39, s. 500). Exempel på kategorier av mottagare kan vara åklagare eller domstol. Om mottagaren finns i ett tredjeland eller är en internationell organisation ska det anges. Vidare ska det framgå hur länge personuppgifterna får behandlas. Om det inte är möjligt att ange hur länge de får behandlas i det enskilda fallet ska i stället kriterierna för att fastställa det anges. Det kan exempelvis vara den föreskrivna tidpunkten i en myndighets registerlagstiftning när de personuppgifter som saken gäller inte längre får behandlas. Den personuppgiftsansvarige ska även underrätta den registrerade om rätten att begära rättelse, radering eller begränsning av behandlingen. Informationen till den enskilde behöver inte omfatta personuppgifter som den sökanden redan tagit del av. Detta följer av 4 kap. 3 § andra stycket brottsdatalagen (Brottsdatalag, 2017/18:232, s.229–234).

För att den enskilde ska kunna hålla sig underrättad om hans eller hennes personuppgifter behandlas och kunna kontrollera om behandlingen utförs författningsenligt bör Säkerhetspolisens nya lag innehålla en bestämmelse som i huvudsak motsvarar 4 kap. 3 § brottsdatalagen. Att en registrerads rätt till information om vilka personuppgifter om honom eller henne som behandlas inte gäller i den utsträckning personuppgifterna inte får lämnas ut behandlas i avsnitt 14.3.1. Personuppgifter i ofärdig text eller som utgör minnesanteckningar behandlas i avsnitt 14.3.2. Vilka närmare krav som bör ställas på en begäran om information kan regleras i förordning.

14.3 Begränsning av rätten till information

14.3.1 Rätten till information får begränsas

Regeringens förslag: Skyldigheten att lämna personrelaterad information ska inte gälla i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning, att uppgifter inte får lämnas ut till den registrerade.

Om det finns grund för att begränsa informationen ska Säkerhetspolisen inte heller vara skyldig att lämna ut skälen för beslut att begränsa informationen eller för beslut i fråga om begäran om rättelse, radering eller begränsning av behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 4 kap. 5 § första stycket brottsdatalagen finns en bestämmelse som begränsar rätten till information. Sådana begränsningar får göras enbart med hänsyn till vissa angivna intressen. Bestämmelser som begränsar rätten till information är nödvändiga för att de behöriga myndigheterna ska kunna utföra sina uppdrag på ett effektivt sätt (prop. 2017/18:232 s. 237). Säkerhetspolisen bör också ha möjlighet att begränsa rätten till information och detta bör därför regleras i den nya lagen. Till skillnad mot vad som gäller enligt brottsdatalagen bör sådana begränsningar inte enbart få göras med hänvisning till vissa angivna intressen. Det kravet ställs upp i direktivet, men bör inte gälla för Säkerhetspolisen. Regleringen bör i stället utformas med 27 § personuppgiftslagen som mönster. Rätten att begränsa eller inte lämna ut personrelaterad information gäller både information som lämnas självmant och på begäran.

I förarbetena till brottsdatalagen konstaterade regeringen att det finns behov av att även kunna begränsa underrättelser om skälen för beslut i fråga om rättelse, radering eller begränsning av behandlingen. Om skälen skulle riskera att röja information som hänför sig till något av de angivna intressena, t.ex. att hemlig avlyssning av elektronisk kommunikation pågår, bör underrättelsen till den registrerade kunna begränsas. Om så inte var fallet skulle enskilda kunna begära rättelse och därigenom få del av information som annars inte skulle lämnas ut (prop. 2017/18:232 s. 240). Även Säkerhetspolisen har behov av att kunna begränsa skälen för besluten i fråga om rättelse, radering eller begränsning av behandlingen. En bestämmelse om detta bör därför tas in i den nya lagen. Att sökanden ska underrättas om sådana beslut kan regleras i förordning.

14.3.2 Ofärdig text och minnesanteckningar

Regeringens förslag: Rätten att få del av personrelaterad information ska inte gälla personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten ska dock gälla om uppgifterna

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

Tredje man ska definieras som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet

och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen föreslår att informationsskyldigheten ska gälla när uppgifterna har lämnats ut till myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Enligt utredningens förslag ska det även följa av bestämmelsen att informationsskyldigheten gäller om uppgifterna behandlas enbart för arkivändamål av allmänt intresse.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* påpekar att definitionen av tredje man inte undantar myndigheter som utövar som utövar tillsyn, kontroll eller revision. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 26 § tredje stycket personuppgiftslagen begränsas informationsskyldigheten. Undantaget gäller för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran om information gjordes eller som utgör minnesanteckning eller liknande. Om uppgifterna redan har lämnats ut till tredje man eller om uppgifterna i den löpande texten ännu inte fått sin slutliga utformning efter ett års behandling, gäller inte undantaget. Det gäller inte heller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål.

Att enskilda inte har någon rätt till insyn i utkast och koncept till skrivelser, beslut och domar under den tid som arbetet pågår värnar myndigheternas verksamhet och skyddar andra enskilda. Av samma skäl är minnesanteckningar eller liknande, t.ex. promemorior eller andra anteckningar som används under handläggningen, fredade från insyn så länge handläggningen pågår.

Utkast under arbete eller minnesanteckningar som inte ska bevaras för framtiden är inte allmänna handlingar enligt 2 kap. tryckfrihetsförordningen och lämnas därmed inte ut enligt offentlighetsprincipen. Det finns därför goda skäl att inte ge en sökande rätt till information om hur hans eller hennes personuppgifter behandlas i ofärdiga texter och minnesanteckningar. Ett undantag för sådan text bör därför tas in i den nya lagen. En motsvarande bestämmelse finns i 4 kap. 6 § brottsdatalagen.

Om personuppgifterna i utkasten har behandlats under längre tid än ett år utan att texten färdigställts väger den registrerades intresse av att kunna ta del av hur personuppgifterna behandlas tyngre än den personuppgiftsansvariges intresse av att fortsätta att behandla personuppgifterna utan insyn. Information om personuppgifterna bör därför lämnas till den registrerade, om inte den personuppgiftsansvarige väljer att i stället radera personuppgifterna i den ofärdiga texten (jfr Personuppgiftslag, prop. 1997/98:44, s. 83 f.).

Om ett utkast eller en minnesanteckning endast används vid statistikproduktion eller för vetenskapliga eller historiska ändamål inom lagens tillämpningsområde bör information om personuppgiftsbehandlingen kunna lämnas. Undantaget bör därför inte gälla för personuppgifter i ofärdiga texter eller minnesanteckningar som enbart behandlas för vetenskapliga, statistiska eller historiska ändamål för de syften som omfattas av lagen. Som utredningen föreslår bör undantaget inte heller gälla

för personuppgifter i utkast eller minnesanteckningar som enbart behandlas för arkivändamål av allmänt intresse. Till skillnad från utredningen anser regeringen dock inte att det behöver framgå av bestämmelsen i lagen. Som anges i avsnitt 12.2.1 faller behandling av personuppgifter för arkivändamål in under dataskyddsförordningen. Att personuppgifter i arkiverade utkast eller minnesanteckningar bör kunna lämnas ut följer av 5 kap. 2 § dataskyddslagen.

Information bör också lämnas om uppgifterna i den ofärdiga texten eller minnesanteckningen har lämnats ut till tredje man. Information bör dock få lämnas till dataskyddsombud, personuppgiftsbiträden och andra personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar behandlar personuppgifter, utan att undantaget upphör att gälla (jfr 26 § tredje stycket andra meningen jämfört med 3 § personuppgiftslagen). För att det ska bli tydligt bör tredje man definieras i lagen som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Definitionen överensstämmer därmed med den definition som finns i brottsdatalagen av tredje man. Som *Säkerhets- och integritetsskyddsnämnden* påpekar bör information även få lämnas till myndigheter som utövar tillsyn, kontroll eller revision utan att undantaget upphör att gälla. Detta bör, på motsvarande sätt som i brottsdatalagen, framgå tydligt av lagtexten.

Det bör alltså i lagen tas in en regel om att information bör lämnas om uppgifter i ofärdig text eller minnesanteckningar har lämnats ut till tredje man, med undantag för myndighet som med stöd av författning utövar tillsyn, kontroll eller revision, om uppgifterna behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller om uppgifterna har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Ett beslut om att begränsa tillgången till denna typ av information får enligt regeringens förslag överklagas till allmän förvaltningsdomstol (avsnitt 16.4.1).

14.3.3 Orimliga eller uppenbart ogrundade framställningar

Regeringens förslag: Om en begäran om personrelaterad information är orimlig eller uppenbart ogrundad får Säkerhetspolisen avslå den.

Om någon begär sådan information eller sådana uppgifter oftare än en gång per år, får Säkerhetspolisen ta ut en rimlig avgift eller avslå begäran.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

En begäran som är orimlig eller uppenbart ogrundad ska avslås

I 4 kap. 7 § första stycket brottsdatalagen föreskrivs att om en begäran om personrelaterad information är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den. Regeringen uttalar i förarbetena till brottsdatalagen att en begäran om information är uppenbart ogrundad om en sökande missbrukar sin rätt till information genom att exempelvis lämna felaktiga eller missvisande uppgifter i sin begäran och orimlig om en sökande utan skäl och vid upprepade tillfällen begär uppgifter. En begäran kan också vara orimlig om sökanden inte lämnar sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen utan ytterligare efterforskningar. Andra omständigheter som kan göra att en begäran anses vara orimlig är att den är så oprecis att det skulle vara närmast omöjligt att besvara den (prop. 2017/18:232 s. 244 f.). Avslagskriterierna i brottsdatalagen överensstämmer med de som anges i artikel 12.5 i dataskyddsförordningen.

Det är av stor praktisk betydelse att Säkerhetspolisen inte åläggs att besvara framställningar som är så obegränsade att det i princip är omöjligt att besvara dem. Säkerhetspolisen bör därför, i likhet med vad som gäller för övriga brottsbekämpande myndigheter, inte vara skyldig att tillgodose en begäran om information som är orimlig eller uppenbart ogrundad. En sådan bestämmelse bör därför tas in i den nya lagen.

En upprepad begäran kan besvaras mot avgift eller avslås

Av 4 kap. 7 § brottsdatalagen följer också att en begäran om information som är orimlig på grund av att den återupprepas antingen kan besvaras mot avgift eller avslås. I förarbetena till brottsdatalagen uttalar regeringen att en ordning med avgiftsfri information en gång per år tillgodoser den enskildes rätt att med rimliga intervall hålla sig underrättad om hans eller hennes personuppgifter behandlas och om behandlingen är författningsenlig. Tidsintervallet är samtidigt anpassat så att den personuppgiftsansvariges arbetsinsats inte blir orimligt betungande. Om information begärs oftare än en gång per år kan det däremot anses som orimligt på grund av att begäran är återkommande. Det ger den enskilde möjlighet att begära information så ofta han eller hon önskar, men tvingar inte den personuppgiftsansvarige att behandla alla framställningar på samma sätt. Den personuppgiftsansvarige får med utgångspunkt i begäran avgöra om den ska besvaras mot avgift eller avslås (prop. 2017/18:232 s. 245).

Även Säkerhetspolisen bör ha möjlighet att ta ut en avgift eller avslå en upprepad begäran om information. En sådan bestämmelse bör därför tas in i den nya lagen och formuleras på motsvarande sätt som i brottsdatalagen. Utgångspunkten bör vara att Säkerhetspolisen i första hand tar ut en rimlig avgift för de kostnader som begäran förorsakar och i andra hand avslå begäran att lämna den informationen. Om myndigheten avser att ta ut avgift för informationen bör den först underrätta sökanden om det och förhöra sig om han eller hon vidhåller sin begäran (jfr. prop. 2017/18:232 s. 245).

Närmare anvisningar för vad som gäller i fråga om avgifter bör kunna meddelas av regeringen eller den myndighet som regeringen bestämmer.

Vad som kan vara en rimlig avgift för att lämna information kan regleras t.ex. i avgiftsförordningen (1992:191).

14.4 Rättelse, radering och begränsning av behandlingen

14.4.1 Rätten till rättelse och komplettering

Regeringens förslag: Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 4 kap. 9 § brottsdatalagen ska den personuppgiftsansvarige på begäran rätta eller komplettera personuppgifter som rör den registrerade om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. En motsvarande skyldighet finns i dag för Säkerhetspolisen i 28 § personuppgiftslagen. Eftersom det är av grundläggande betydelse både för Säkerhetspolisens verksamhet och för enskilda att de personuppgifter som behandlas är korrekta bör en motsvarande bestämmelse införas i Säkerhetspolisens nya lag. Den bör utformas som i brottsdatalagen. Skyldigheten för Säkerhetspolisen att självmant vidta åtgärder när det upptäcks att personuppgifter är felaktiga, ofullständiga eller inaktuella behandlas i avsnitt 9.3.

Att en felaktig eller ofullständig personuppgift rättas eller kompletteras kan innebära att den ersätts av en annan uppgift som är korrekt ur ett objektivt perspektiv eller kompletteras med en uppgift om de rätta förhållandena så att den blir fullständig i objektiv mening. Det kan vara fråga om t.ex. ett felaktigt namn eller att endast delar av ett namn har återgetts i en handling. Det kan även vara fråga om något fel som uppstått på grund av ett tekniskt förfarande. Det ska alltså röra sig om ett fel eller en ofullständighet på grund av något som inte bygger på en bedömning. En felaktig uppgift kan också rättas på det sättet att den tas bort utan att ersättas.

14.4.2 Rätten till radering

Regeringens förslag: På begäran av den registrerade ska Säkerhetspolisen utan onödigt dröjsmål radera personuppgifter som rör honom eller henne om de behandlas på otillåtet sätt. Detsamma gäller om det krävs radering för att Säkerhetspolisen ska utföra en rättslig förpliktelse.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I brottsdatalagen finns, förutom en möjlighet för den registrerade att begära rättelse, även en möjlighet att begära radering om personuppgifterna behandlas i strid med lagen. Detta regleras i 4 kap. 10 §. I dag är Säkerhetspolisen skyldig att på begäran av den registrerade bl.a. utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen. Detta följer av 28 § personuppgiftslagen. En motsvarande bestämmelse bör införas i Säkerhetspolisens nya lag. Den bör utformas som i brottsdatalagen.

Hur personuppgifter ska behandlas diskuteras i avsnitt 8 och 9. Där föreslås att det i lagen ska tas in bestämmelser om att personuppgifter ska vara adekvata och relevanta, att inte fler personuppgifter än nödvändigt får behandlas, att de bara får behandlas om det finns en rättslig grund och för särskilt angivna ändamål. Vidare föreslås att det ska regleras i vilken utsträckning känsliga personuppgifter får behandlas och hur länge personuppgifter får behandlas. Frågan om en personuppgift bör raderas får bedömas mot bakgrund av dessa bestämmelser. Vid bedömningen ska även 2 kap. tryckfrihetsförordningen och det arkivrättsliga regelverket beaktas.

Enligt brottsdatalagen får den registrerade även begära att en personuppgift ska raderas om det krävs för att utföra en rättslig förpliktelse. Motsvarande bör gälla även i Säkerhetspolisens nya lag. En rättslig förpliktelse kan t.ex. vara ett föreläggande från tillsynsmyndigheten om att uppgifter ska raderas.

14.4.3 Begränsning av behandlingen

Regeringens förslag: Om förutsättningarna för att radera personuppgifter är uppfyllda, men uppgifterna behöver finnas kvar av bevisskäl, ska Säkerhetspolisen på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av dem.

Om den registrerade bestrider att personuppgifter som rör honom eller henne är korrekta och det inte kan fastställas, ska Säkerhetspolisen utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för regeringens förslag

Begränsning när personuppgifterna behöver finnas kvar av bevisskäl

I 4 kap. 10 § andra stycket brottsdatalagen föreskrivs att om förutsättningarna för att radera personuppgifter är uppfyllda, men uppgifterna behöver finnas kvar av bevisskäl, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av dem. Det kan då ligga både i den registrerades och i det allmännas intresse att personuppgifter sparas en tid som bevisning om hur de har behandlats i stället för att raderas. En motsvarande bestämmelse bör även införas i Säkerhetspolisens nya lag.

Ett exempel på att personuppgifter har sparats av bevisskäl är det s.k. kringresanderegistret där uppgifter enligt Säkerhets- och integritetsskyddsnämnden (uttalande den 15 november 2013, dnr 173–2013) behandlades i strid med polisdatalagen och där uppgifterna därför togs bort. Två kopior sparades dock för att Polismyndigheten skulle kunna besvara frågor om vilka som förekom i registret och för att uppgifterna eventuellt skulle kunna användas som bevis (se bl.a. SOU 2015:39 s. 574 och 645 f.).

Begränsning när personuppgifternas korrekthet bestrids

Begränsning av behandlingen kan också, enligt 4 kap. 9 § andra stycket brottsdatalagen, komma i fråga om den registrerade bestrider att personuppgifterna är korrekta, men det inte är möjligt att fastställa om så är fallet. En felaktig personuppgift ska utan onödigt dröjsmål rättas enligt brottsdatalagen. Om den personuppgiftsansvariges utredning om den omstridda personuppgiften inte kan slutföras tillräckligt snabbt ska behandlingen begränsas under utredningstiden. Uppgifterna får då inte behandlas av den personuppgiftsansvarige eller personuppgiftsbiträden annat än för det ändamål som föranledde begränsningen. Om det efter utredning visar sig att personuppgifterna är korrekta kan behandlingen av dem fortsätta som tidigare. Begränsningen ska då upphävas. Innan dess ska dock den registrerade underrättas om att begränsningen upphör. Skulle det visa sig att personuppgifterna är felaktiga ska den personuppgiftsansvarige rätta dem, varefter begränsningen kan upphöra. Åtgärden kan inte vara ett alternativ till radering, eftersom den ska användas när uppgifters korrekthet bestrids och därför knyter an till rättelseförfarandet (prop. 2017/18:232 s. 252). Även denna typ av begränsning bör införas i Säkerhetspolisens nya datalag. Bestämmelsen bör utformas som i brottsdatalagen.

Åtgärd som visar att behandlingen har begränsats

Säkerhetspolisen ska vidta en åtgärd med personuppgifterna som visar att behandlingen har begränsats. Hur själva begränsningen bör göras får dock bedömas med utgångspunkt i vad som är lämpligt i det enskilda fallet. En naturlig åtgärd kan vara att avskilja uppgifterna från det datasystem där de behandlas. Begränsningen kan också ha formen av en teknisk begränsning, vilket kan vara en lämplig åtgärd medan personuppgifternas korrekthet utreds. En tredje möjlighet att begränsa behandlingen är att inskränka tillgången till uppgifterna.

Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av vare sig den personuppgiftsansvarige eller ett personuppgiftsbiträde utom för det syfte som har föranlett begränsningen. Har en personuppgift behandlats på otillåtet sätt måste den ändå kunna behandlas inom ramen för en utredning av om brott har begåtts i samband med behandlingen eller om någon tjänsteman vid behandlingen gjort sig skyldig till fel som kan föranleda disciplinansvar eller skadestånd. Det beror på felets karaktär om all behandling av personuppgiften måste upphöra eller om det bara gäller behandlingen i viss verksamhet. Vidare bör beaktas att nationella bestämmelser om

straffrättsliga förfaranden kan påverka rätten till begränsning av behandling (prop. 2017/18:232 s. 252 f.).

Oavsett vilken åtgärd som vidtas för att begränsa behandlingen är den inte avsedd att vara permanent. När personuppgifterna inte längre behöver finnas kvar som bevisning ska de raderas och när utredningen om personuppgifternas korrekthet är avslutad ska begränsningen av behandlingen upphöra och uppgifterna antingen fortsätta att behandlas eller rättas. Begränsning av behandlingen bör i likhet med de andra korrigerande åtgärderna genomföras utan onödigt dröjsmål.

14.4.4 Val av åtgärd

Regeringens förslag: Säkerhetspolisen avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt förarbetena till personuppgiftslagen väljer den personuppgiftsansvarige själv vilket alternativ som ska användas av rättelse, utplånande eller blockering (prop. 1997/98:44 s. 87). Den ordningen gäller även i fråga om rättelse, radering eller begränsning av behandlingen enligt brottsdatalagen (4 kap. 11 §). Den personuppgiftsansvarige ska därför enligt brottsdatalagen inte endast pröva om den åtgärd som begärs av den registrerade ska vidtas eller inte, utan är fri att välja en annan åtgärd om den är lämpligare. Det följer av att den personuppgiftsansvarige är skyldig att vidta alla rimliga åtgärder för att rätta personuppgifter som är felaktiga eller ofullständiga och för att radera eller begränsa behandlingen av personuppgifter som har behandlats otillåtet. Den personuppgiftsansvarige ska alltså se till att den lämpligaste åtgärden vidtas oavsett vad som begärs. En åtgärd kan emellertid inte vidtas om den strider mot annan lagstiftning. Det innebär t.ex. att en myndighet inte kan radera uppgifter i en allmän handling utan författningsstöd för gallring (prop. 2017/18:232 s. 253 f.).

Även Säkerhetspolisen bör få avgöra vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen. En bestämmelse som motsvarar 4 kap. 11 § brottsdatalagen bör därför tas in i Säkerhetspolisen nya lag.

14.5 Information ska inte avgiftsbeläggas

Regeringens förslag: Information om behandlingen av personuppgifter som Säkerhetspolisen ska lämna på eget initiativ ska lämnas utan avgift. Information som ska lämnas på begäran är avgiftsfri en gång per år.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om förslaget.

Skälen för regeringens förslag: På samma sätt som för övriga brottsbekämpande myndigheter bör den information som Säkerhetspolisen lämnar som huvudregel vara kostnadsfri. En bestämmelse som anger det bör därför, som utredningen föreslår, tas in i den nya lagen. Den bör formuleras på samma sätt som 4 kap. 12 § brottsdatalagen. Säkerhetspolisen ges då möjlighet att ta ut avgift för personrelaterad information om sådan begärs oftare än en gång per år.

15 Tillsyn

15.1 Det behövs en särskild reglering

15.1.1 Dagens tillsyn över Säkerhetspolisens personuppgiftsbehandling

I dag utövas tillsynen över Säkerhetspolisens behandling av personuppgifter i den brottsbekämpande verksamheten både av Datainspektionen och Säkerhets- och integritetsskyddsnämnden (i fortsättningen nämnden). Datainspektionen utövar också tillsyn över Polismyndighetens och övriga brottsbekämpande myndigheters behandling av personuppgifter, medan nämnden även utövar tillsyn över Polismyndighetens och Ekobrottsmyndighetens behandling av personuppgifter. Enligt övergångsbestämmelserna till dataskyddslagen och polisens brottsdatalag gäller fortfarande regleringen i personuppgiftslagen (1998:204) för Datainspektionens tillsyn över Säkerhetspolisens personuppgiftsbehandling på området för nationell säkerhet. För nämndens motsvarande tillsyn över Säkerhetspolisen gäller övergångsvis äldre föreskrifter i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Datainspektionens uppgift är att bl.a. arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter. Av hänvisningarna i 2 kap. 2 § första stycket 11 och 13 och 6 kap. 4 § 1 polisdatalagen (2010:361) följer att personuppgiftslagens bestämmelser om tillsyn är tillämpliga i Säkerhetspolisens brottsbekämpande verksamhet. Detta innebär att inspektionen har rätt att för sin tillsyn få tillgång till personuppgifter, upplysningar och dokument och tillträde till lokaler som används för behandling av personuppgifter (43 § personuppgiftslagen). Genom påpekanden och liknande förfaranden ska inspektionen i första hand försöka åstadkomma rättelse och i andra hand besluta om förbud mot annan behandling än lagring (45 § personuppgiftslagen) eller vid domstol ansöka om utplåning av personuppgifter som behandlats på ett olagligt sätt (47 § personuppgiftslagen). I vissa fall kan inspektionen förena sina förelägganden med vite (44 § personuppgiftslagen). Om en annan myndighet har behörighet att utöva tillsyn avstår Datainspektionen normalt från att utöva tillsyn på det området (Ett samlat ansvar för tillsyn över den personliga integriteten, SOU 2016:65, s. 79).

Enligt lagen om tillsyn över viss brottsbekämpande verksamhet utövar nämnden tillsyn över den behandling av personuppgifter enligt polisdatalagen som utförs av Säkerhetspolisen. Tillsynen ska särskilt avse behandling av känsliga personuppgifter. Tillsynen över Säkerhetspolisen omfattar även behandling enligt den tidigare gällande polisdatalagen (1998:622). Nämnden utövar också tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Nämnden utövar sin tillsyn genom inspektioner och andra undersökningar, som kan vara både föranmälda och oanmälda. Nämnden ska också på begäran av enskilda kontrollera om de har varit föremål för behandling av personuppgifter inom nämndens tillsynsområde och underrätta dem om att kontrollen genomförts. Nämnden har för sin tillsyn rätt att få tillgång till de uppgifter och den hjälp som den begär av den myndighet som tillsynen avser. Om nämnden finner något att anmärka på får den lämna synpunkter på hur bristerna bör avhjälpas. Nämndens rekommendationer är inte bindande och kan inte överklagas.

Om nämnden upptäcker brott ska det enligt 20 § nämndens instruktion anmälas till Åklagarmyndigheten och om den finner något som kan leda till skadeståndsansvar för staten ska det anmälas till Justitiekanslern. Finner nämnden omständigheter som Datainspektionen bör uppmärksammas på, ska det anmälas till inspektionen.

Riksdagens ombudsmän (JO) och Justitiekanslern utövar tillsyn över hur lagar och andra föreskrifter tillämpas i offentlig verksamhet. Deras tillsyn omfattar därmed även behandlingen av personuppgifter och skyddet av enskildas personliga integritet vid sådan behandling. Både JO och Justitiekanslern är extraordinära tillsynsorgan.

15.1.2 Utgångspunkter för överväganden om tillsyn

Frågor om tillsyn har fått ökat fokus

Frågor om tillsyn, t.ex. hur den ska bedrivas och vem som ska utöva tillsyn, har diskuterats inom många olika områden under senare år och lösningarna varierar. Regeringen har i skrivelsen En tydlig, rättssäker och effektiv tillsyn (skr. 2009/10:79, i det följande tillsynsskrivelsen) utvecklat sin syn på tillsynsfrågor. I skrivelsen framhålls att den offentliga tillsynen är viktig för att stärka efterlevnaden av de föreskrifter som riksdagen och regeringen har beslutat. Tillsynen bidrar till att upprätthålla grundläggande värden i samhället som bl.a. rättssäkerhet. Medborgarna ska genom tillsynen vara tillförsäkrade att deras intressen tas till vara.

Utgångspunkten i skrivelsen är att det krävs större enhetlighet i fråga om tillsyn. I skrivelsen framhålls bl.a. att den offentliga tillsynen bör präglas av tydlighet och enhetlighet. Ett sätt att uppnå det är att tillsynsmyndigheternas uppdrag preciseras i form av tillsynsuppgifter, regler och, i förekommande fall, mål och prioriteringar. I skrivelsen pekas också på behovet av enhetliga begrepp.

Vidare understryks att avsteg från de generella bedömningarna i skrivelsen kan leda till minskad tydlighet och enhetlighet, men att det inom vissa områden ändå kan finnas skäl att göra avsteg om det leder till en mer ändamålsenlig tillsyn inom det specifika området (skr. 2009/10:79 s. 13).

En fri och oberoende tillsyn måste värnas

Ett led i en effektivare tillsyn är, som framhålls i tillsynsskrivelsen, att skapa tydliga regler för verksamheten så att såväl tillsynsmyndigheten och tillsynsobjekten som enskilda som befarar att deras personuppgifter kan ha behandlats på ett otillåtet sätt vet vilka skyldigheter respektive rättigheter de har och vilka resultat som kan förväntas av tillsynen. Samtidigt är det lika viktigt att inte skapa detaljregler som riskerar att begränsa tillsynsmyndighetens möjligheter att arbeta oberoende och att prioritera bland sina arbetsuppgifter på det sätt som den anser bäst gagnar tillsynsverksamheten som helhet. Det är alltså en balansgång mellan att skapa tydliga regler och att inte åstadkomma ett regelsystem som riskerar att hämma tillsynsmyndighetens oberoende. Regeringens utgångspunkt är att en effektiv tillsyn bäst gagnas av att den som utövar tillsynen får så stor frihet att välja arbetsformer som möjligt, utan att avkall görs på rättssäkerheten. Den flexibilitet som den nuvarande tillsynsverksamheten ger bör därför så långt möjligt värnas.

Utredningen om tillsynen över den personliga integriteten

Utredningen om tillsynen över den personliga integriteten har bl.a. haft i uppdrag att kartlägga vilken tillsyn över behandling av personuppgifter som bedrivs i dag och överväga om den i större utsträckning kan samlas hos en myndighet. (dir. 2014:164). Utredningen föreslog i sitt betänkande att tillsynen över Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten även fortsättningsvis skulle utövas av både Datainspektionen och nämnden (Ett samlat ansvar för tillsyn över den personliga integriteten, SOU 2016:65, s. 175 f. och 189). Utredningen föreslog också att nämnden inte längre skulle utöva tillsyn över Polismyndighetens personuppgiftsbehandling. I förarbetena till brottsdatalagen tog dock regeringen ställning för att nämnden även fortsättningsvis ska utöva tillsyn över Polismyndighetens personuppgiftsbehandling på samma sätt som i dag och inte enbart utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling (Brottsdatalag, prop. 2017/18:232, s. 271).

I 5 kap. brottsdatalagen (2018:1177) regleras i dag vilka uppgifter och befogenheter tillsynsmyndigheten har och hur tillsynen ska bedrivas över de brottsbekämpande myndigheterna.

Tillsynsverksamhet över Säkerhetspolisen fyller en viktig kontrollfunktion

För verksamheten vid Säkerhetspolisen gäller i stor utsträckning sekretess och allmänheten och enskilda har begränsad insyn i den. Det innebär bl.a. att enskilda inte på samma sätt som i annan verksamhet kan reagera över felaktigheter eller komma med allmänna klagomål över hur verksamheten bedrivs. Den kontroll som allmänhetens tillgång till allmänna handlingar normalt innebär för offentlig verksamhet ger, på grund av den omfattande sekretessen, därmed inte samma effekt som i annan verksamhet. Tillsynsverksamheten fyller därför en viktig kontrollfunktion.

På samma sätt som i dag bör personuppgiftsbehandling som rör nationell säkerhet stå under tillsyn och en utgångspunkt bör vara att tillsynen inte ska försämras. Eftersom all Säkerhetspolisens operativa verksamhet anses

vara i någon mening brottsbekämpande talar det för att regleringen bör efterlikna brottsdatalagens bestämmelser om tillsyn.

15.1.3 Tillsynen över Säkerhetspolisen bör regleras i den nya lagen

Regeringens förslag: Tillsynen över Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet ska regleras i Säkerhetspolisens datalag.

Utredningens förslag överensstämmer med regeringens förslag.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 1 kap. 4 § brottsdatalagen gäller lagen inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Den gäller inte heller för Polismyndigheten när myndigheten övertagit en arbetsuppgift från Säkerhetspolisen som rör nationell säkerhet. Nationell säkerhet har också undantagits från dataskyddsförordningens tillämpningsområde (avsnitt 7.1). Förordningens bestämmelser om tillsyn är därför inte anpassade till sådan verksamhet. Det är därmed nödvändigt att särreglera tillsynen över Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet. Det bör därför i den nya lagen regleras vilken tillsyn som ska utövas över den personuppgiftsbehandling som förekommer enligt lagen.

15.2 Vem ska utöva tillsyn över Säkerhetspolisen?

Regeringens bedömning: Tillsynen över Säkerhetspolisens behandling av personuppgifter bör utövas av både Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Deras tillsyn bör i huvudsak vara densamma som i dag.

Utredningens bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: *Datainspektionen* tillstyrker utredningens förslag att tillsynen över Säkerhetspolisen bör utövas av både inspektionen och nämnden. *Säkerhetspolisen* anser att frågan om parallell tillsyn och hur den kan lösas bör behandlas i särskild ordning eftersom den kräver en djupare analys än vad tiden för den nu aktuella utredningen har medgett.

Skälen för regeringens bedömning

För- och nackdelar med parallell tillsyn

En första fråga att ta ställning till är om dagens parallella tillsyn över Säkerhetspolisens personuppgiftsbehandling bör bestå eller om tillsynen bör utföras av en tillsynsmyndighet.

En fördel med parallell tillsyn är att myndigheterna kan inrikta sin granskning på olika områden, vilket kan bidra till en mer omfattande och allsidig tillsyn. Två tillsynsmyndigheter med olika uppdrag och fokus kan på så sätt komplettera varandra. En sådan förstärkt tillsyn har ansetts vara

särskilt värdefull i verksamhet som omfattas av stark sekretess och där allmänheten och enskilda har begränsad insyn (Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m., prop. 2006/07:133, s. 30 f., Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 273 f. och SOU 2016:65 s. 175 f.).

Nackdelarna med parallell tillsyn är att det kan leda till oklar ansvarsfördelning mellan tillsynsmyndigheterna. Det finns då risk för att vissa frågor aldrig blir föremål för tillsyn eller att samma fråga granskas gång på gång. Även om myndigheterna har olika fokus och inriktning på sin tillsyn kan parallell tillsyn vidare leda till motstridig praxis. Ett överlappande ansvar riskerar också att medföra dubbelarbete och skapa samordningsbehov och därmed inte vara resurseffektivt (Riksrevisionens rapport om Säkerhets- och integritetsskyddsnämndens tillsyn över brottsbekämpande myndigheter, skr. 2015/16:188, s. 31 f.). En särskild nackdel med parallell tillsyn är att den kan leda till att fler personer får insyn i speciellt känslig verksamhet där hemliga uppgifter hanteras i stor omfattning.

Det finns således både för- och nackdelar med parallell tillsyn. För att kunna besvara frågan om den parallella tillsynen bör bestå eller om tillsynen bör utövas av en myndighet måste för- respektive nackdelarna med de myndigheter som är aktuella för tillsynsuppdraget, dvs. Datainspektionen och nämnden, belysas närmare.

För- och nackdelar med nämnden som tillsynsmyndighet

Nämnden inrättades bl.a. för att förstärka tillsynen över Säkerhetspolisen. Nämndens särskilda beslutsform, med parlamentarisk förankring, har ansetts utgöra dess styrka och vara särskilt viktig för att tillgodose allmänhetens insyn i verksamhet som omfattas av stark sekretess (prop. 2006/07:133 s. 65 och prop. 2009/10:85 s. 272 f.). Bestämmelserna i 42 kap. offentlighets- och sekretesslagen (2009:400) om sekretess hos nämnden har också anpassats till behovet av att kunna hantera hemliga uppgifter i tillsynen. Regeringen har framhållit att nämnden har särskild insikt i och erfarenhet av sådan verksamhet som nu är i fråga. Det ökar, enligt förarbetena till polisdatalagen, förutsättningarna för att tillsynen inriktas på de områden där det finns särskilda risker för intrång i enskildas integritet (prop. 2009/10:85 s. 273 f.).

Det som särskilt talar för att välja nämnden som tillsynsmyndighet är därför dess särskilda kompetens, erfarenhet och vana att utöva tillsyn över personuppgiftsbehandling i känslig verksamhet där sekretessen är mycket omfattande. Förutom att ha god kännedom om den verksamhet som tillsynen avser är nämnden också väl förtrogen med den personuppgiftsbehandling som utförs och vilka personuppgiftssamlingar som förs av Säkerhetspolisen. En annan fördel är att nämnden har ett begränsat tillsynsuppdrag, vilket ger den goda förutsättningar att säkerställa att tillsyn över Säkerhetspolisen bedrivs på ett aktivt och kontinuerligt sätt. En ytterligare omständighet som talar för nämnden som tillsynsmyndighet är att det endast är nämnden som har till uppdrag att utföra en kontroll på begäran av en enskild avseende Säkerhetspolisens personuppgiftsbehandling. Nämnden utövade i praktiken länge ensam

tillsynen över Säkerhetspolisen. Riksrevisionen har granskat verksamheten och funnit att nämnden utför sina uppgifter på ett ändamålsenligt sätt (skr. 2015/16:188 s. 3). Sekretessregleringen är också särskilt anpassad för tillsynen över Säkerhetspolisen.

Det som kan tala mot att nämnden ensam utses till tillsynsmyndighet är att den är liten och därmed sårbar för personalförändringar, vilket kan leda till att värdefull erfarenhet går förlorad. Ur ett säkerhetsperspektiv kan det samtidigt vara en fördel att nämnden är liten, eftersom det innebär att färre personer blir involverade i tillsynen.

Det som vidare talar mot att välja nämnden som enda tillsynsmyndighet är att den i dag inte har de befogenheter som krävs för att utöva tillsynen på egen hand, Det är också tveksamt om det är lämpligt att ge nämnden sådana befogenheter med hänsyn till hur nämnden är organiserad. Vidare får nämndens avgöranden inte överklagas. Samtidigt talar starka skäl för att det bör finnas möjlighet att klaga på vissa av tillsynsmyndighetens beslut eftersom de kan få långtgående konsekvenser för tillsynsobjektet.

För- och nackdelar med Datainspektionen som tillsynsmyndighet

Det som särskilt talar för att välja Datainspektionen som tillsynsmyndighet är att den har bred kompetens och lång erfarenhet av tillsyn över hur personuppgifts- och integritetsskyddslagstiftning tillämpas. Inspektionen har därför goda förutsättningar att utöva tillsyn över tillämpningen av allmänna principer för behandling av personuppgifter. Eftersom inspektionen utövar tillsyn över övriga brottsbekämpande myndigheter får den också en allmän överblick som nämnden saknar.

Datainspektionen har ett generellt uppdrag att följa den tekniska utvecklingen på personuppgiftsområdet. Inspektionen genomför också förhandssamråd med de flesta myndigheter och andra personuppgiftsansvariga. Genom samarbetet inom EU kommer inspektionen att få en överblick över den tekniska utvecklingen även i andra stater. Det skapar goda förutsättningar för rådgivning i frågor som gäller uppbyggnad av it-system.

Det som främst talar mot att välja Datainspektionen som enda tillsynsmyndighet är att inspektionen har ett mycket omfattande tillsynsuppdrag och att tillsynen över en viss myndighet därför av naturliga skäl bara kan ägnas begränsade resurser. Inspektionen utövade i praktiken länge inte någon tillsyn över Säkerhetspolisen och har därför inte samma kunskap som nämnden om Säkerhetspolisens verksamhet och personuppgiftsbehandling. Genom EU:s dataskyddsreform har inspektionen dessutom fått ett utökat uppdrag som kan medföra att utrymmet att bedriva tillsyn över enskilda myndigheter i praktiken begränsas ytterligare.

Den parallella tillsynen bör bestå

Vilken myndighet bör då utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling? Som konstaterats finns det både för- och nackdelar med ett parallellt tillsynssystem och det finns både för- och nackdelar med att välja Datainspektionen respektive nämnden som ensam tillsynsmyndighet. Som utredningen konstaterar kompletterar myndigheternas styrkor varandra. Detta lyfts också som argument av

Utredningen om tillsyn över den personliga integriteten för att nämnden, vid sidan av Datainspektionen, ska fortsätta att ha tillsyn över Säkerhetspolisens personuppgiftsbehandling (SOU 2016:65 s. 179). En sådan ordning överensstämmer också med den tillsyn som i dag utövas över Polismyndighetens personuppgiftsbehandling. Tillsynen över Säkerhetspolisens personuppgiftsbehandling skulle vidare minska betydligt i omfattning om den parallella tillsynen skulle upphöra, eftersom det inte är realistiskt att förvänta sig att Datainspektionens tillsyn skulle kunna ersätta den omfattande tillsyn som i dag utövas av nämnden. Tillsynen över Säkerhetspolisens personuppgiftsbehandling bör mot den bakgrunden fortsätta att vara parallell och utövas av både Datainspektionen och nämnden. Vad *Säkerhetspolisen* anfört i denna del föranleder ingen annan bedömning.

15.3 Det behövs inte någon definition av tillsynsmyndighet i lagen

Regeringens förslag: Det ska införas en bestämmelse i lagen som upplyser om att regler om Säkerhets- och integritetsskyddsnämndens tillsyn över Säkerhetspolisens personuppgiftbehandling finns i lagen om tillsyn över viss brottsbekämpande verksamhet.

Regeringens bedömning: Det behöver inte införas en definition av tillsynsmyndighet i lagen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att det ska införas en definition av tillsynsmyndighet.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag och bedömning: Att det infördes en definition av tillsynsmyndighet i brottsdatalagen var för att det krävdes enligt dataskyddsdirektivet. Motsvarande behov finns inte i Säkerhetspolisens nya datalag och en sådan definition behöver därför inte införas i lagen. Däremot bör Datainspektionen pekas ut som tillsynsmyndighet över Säkerhetspolisens personuppgiftsbehandling enligt lagen. Detta kan göras på förordningsnivå. Att även nämnden är tillsynsmyndighet kommer att framgå av lagen om tillsyn över viss brottsbekämpande verksamhet (avsnitt 15.7). En bestämmelse som upplyser om att regler om nämndens tillsyn över Säkerhetspolisens personuppgiftsbehandling finns i lagen om tillsyn över viss brottsbekämpande verksamhet bör, av tydlighetsskäl, tas in i lagen.

15.4 Tillsynsmyndighetens uppgifter

15.4.1 Allmän tillsyn

Regeringens förslag: Tillsynsmyndigheten ska utöva allmän tillsyn över Säkerhetspolisens personuppgiftsbehandling.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* välkomnar förslaget i denna del. *Säkerhetspolisen* anser att det bör införas en bestämmelse i den nya lagen som motsvarar 5 kap. 1 § brottsdatalagen om tillsynsmyndighetens uppdrag. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 5 kap. 2 § 1 brottsdatalagen ska tillsynsmyndigheten utöva allmän tillsyn över personuppgiftsbehandling. På motsvarande sätt som i brottsdatalagen bör det av Säkerhetspolisens nya lag framgå att tillsynsmyndigheten ska utöva allmän tillsyn. Med detta avses rättslig tillsyn över hur Säkerhetspolisen följer regelverket för behandling av personuppgifter. Sådan tillsyn har av naturliga skäl främst ett tillbakablickande perspektiv. Den inriktas i första hand på att kontrollera om behandlingen av personuppgifter är författningsenlig och utförs normalt genom granskning av dokumentation och inspektioner på plats.

Uppgiften att bedriva allmän tillsyn över Säkerhetspolisens personuppgiftsbehandling kräver delvis andra överväganden än tillsynen över andra brottsbekämpande myndigheters personuppgiftsbehandling. Det beror på att tillsynen, som beskrivs i avsnitt 15.1.2, inte i samma utsträckning som annars kan bygga på klagomål från allmänheten och mediegranskning. Den allmänna tillsynen måste i stället bygga på att de som utövar tillsyn har goda kunskaper om både verksamheten och de risker för den personliga integriteten som personuppgiftsbehandlingen kan föra med sig.

En särskild fråga är om tillsynen bör omfatta både Säkerhetspolisen och eventuella personuppgiftsbiträden som myndigheten anlitar. När det gäller Säkerhetspolisens verksamhet är de faktiska möjligheterna att låta personuppgiftsbiträden hantera personuppgifter i den operativa verksamheten betydligt mer begränsade än i annan brottsbekämpande verksamhet på grund av sekretessens omfattning. Behovet av att låta tillsynen omfatta personuppgiftsbiträden är därmed begränsat. Det finns emellertid inte skäl att ha en annan lösning för tillsynen enligt Säkerhetspolisens datalag än den som gäller för andra brottsbekämpande myndigheter. Tillsynen bör således även omfatta personuppgiftsbehandling som personuppgiftsbiträden utför enligt lagen.

Säkerhetspolisen anser att det i den nya lagen bör införas en bestämmelse som motsvarar 5 kap. 1 § brottsdatalagen om tillsynsmyndighetens uppdrag. I paragrafen föreskrivs att tillsynsmyndigheten ska verka för att både fysiska personers grundläggande rättigheter och friheter skyddas i samband med personuppgiftsbehandling och för att underlätta det fria flödet av personuppgifter inom ramlagens område. Att bestämmelsen infördes i brottsdatalagen berodde på att dataskyddsdirektivet krävde det. Något motsvarande krav finns inte här. Vidare kan de dubbla syften som anges i brottsdatalagens bestämmelse komma att strida mot varandra i vissa fall. Mot den bakgrunden och då utredningen inte har föreslagit att det införs en sådan bestämmelse, ser inte heller regeringen skäl för att det tas in en motsvarande bestämmelse i den nya lagen.

15.4.2 Förhandssamråd och annat råd och stöd

Regeringens förslag: Tillsynsmyndigheten ska vid förhandssamråd och när det i övrigt är påkallat ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Utredningens förslag överensstämmer i sak med regeringen.

Remissinstanserna: *Datainspektionen* tillstyrker utredningens förslag att Säkerhetspolisen endast ska samråda med inspektionen, men att Datainspektionen inom ramen för samrådet ska låta nämnden yttra sig om det är lämpligt. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Dagens samrådsskyldighet

Enligt 2 § polisdataförordningen ska Säkerhetspolisen samråda med Datainspektionen i god tid innan beslut fattas om nya it-system av större omfattning eller betydande förändringar genomförs i befintliga it-system om de kan innebära särskilda risker för intrång i den personliga integriteten. Om det krävs ska Säkerhetspolisen även samråda med nämnden.

Säkerhetspolisen samråder normalt med båda myndigheterna. Deras rådgivning skiljer sig åt på så sätt att Datainspektionen lämnar mer omfattande och generella synpunkter, medan nämndens uttalanden oftast är kortare och riktar in sig mer på konkreta frågor om person-uppgiftsbehandlingen. Den dubbla samrådsskyldigheten har kritiserats eftersom det finns risk att tillsynsmyndigheterna lämnar motstridiga råd (jfr skr. 2015/16:188 s. 31 f.).

Tillsynsmyndighetens skyldigheter vid förhandssamråd

I avsnitt 13.2.5 föreslås att Säkerhetspolisen ska samråda med tillsynsmyndigheten om en konsekvensbedömning visar särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång. Förhandssamrådet motsvarar i stort det samråd som regleras i 2 § polisdataförordningen.

Tillsynsmyndighetens skyldigheter vid samråd är i dag inte närmare reglerade. Som framgår av avsnitt 13.2.5 bör Säkerhetspolisens skyldigheter vid förhandssamråd regleras på samma sätt som i brottsdata-lagen. Tillsynsmyndigheten bör då också ha i huvudsak motsvarande skyldigheter. Det innebär att tillsynsmyndigheten bör vara skyldig att lämna skriftliga råd i vissa fall. Den närmare utformningen av tillsynsmyndighetens skyldigheter vid förhandssamråd kan dock regleras på lägre författningsnivå.

Nämndens roll vid förhandssamråd

Frågan är om Säkerhetspolisen även i fortsättningen bör ha samma skyldighet att samråda med nämnden som i dag.

Nämndens tillsynsuppdrag avser rättslig granskning i efterhand och uttalanden om behov av förändringar i verksamheten eller i lagstiftningen.

I förarbetena framhålls att planerade åtgärder inte kan bli föremål för granskning och att nämndens verksamhet således inte kan uppfattas som ett godkännande av framtida åtgärder (prop. 2006/07:133 s. 63). Även om tyngdpunkten i nämndens tillsyn alltjämt kommer att vara tillsyn i efterhand bör nämnden inte stängas ute vid överväganden som kan komma att påverka den framtida personuppgiftsbehandlingen. Eftersom Datainspektionens och nämndens kompetens och erfarenheter kompletterar varandra anser regeringen, i likhet med utredningen, att nämnden även i fortsättningen bör ha en roll vid förhandssamråd.

Det är dock inte lämpligt att behålla den dubbla samrådsskyldigheten som den är utformad i dag. I stället bör inspektionen, om det är lämpligt, ge nämnden tillfälle att yttra sig inom ramen för förhandssamrådet. Nämnden bör då också ha rätt att ta del av underlaget för förhandssamrådet. Nämnden får på det sättet möjlighet att lämna synpunkter utan att det uppfattas som ett godkännande av viss behandling på förhand. Den lösningen innebär att risken för att Säkerhetspolisen får motstridiga råd kan undvikas. Skulle Säkerhetspolisen föreslå att Datainspektionen låter nämnden yttra sig bör inspektionen givetvis beakta det. Detta kan regleras på förordningsnivå.

Annat råd och stöd

En viktig uppgift vid tillsyn är att tillsynsmyndigheten även i andra fall än vid förhandssamråd lämnar råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lagstiftningen. Att tillsynsmyndigheten har en sådan uppgift framgår därför i dag av 5 kap. 4 § brottsdatalagen. Eftersom Säkerhetspolisen har samma behov som andra brottsbekämpande myndigheter av att rådgöra med tillsynsmyndigheten, bör tillsynsmyndigheten ha samma rådgivande uppgifter som anges i brottsdatalagen. Av hänsyn till tillsynsmyndighetens oberoende bör bestämmelsen utformas så att det, förutom vid förhandssamråd, tydligt framgår att myndigheten själv avgör när råd och stöd kan vara påkallat.

15.5 Tillsynsmyndighetens befogenheter

15.5.1 Undersökningsbefogenheter

Regeringens förslag: Tillsynsmyndigheten ska ha rätt att av Säkerhetspolisen och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: Rättslig tillsyn består till stor del av granskning av dokumentation. Tillsynsmyndigheten behöver därför tillgång till de personuppgifter som behandlas. Tillsynsmyndigheten behöver även upplysningar och dokumentation om pågående behandlingar. Därutöver bör tillsynsmyndigheten ha rätt till annan information, bl.a. dokumentation av säkerhets- och skyddsåtgärder samt dokumentation som inte är direkt kopplad till den behandling som granskas, men som tillsynsmyndigheten ändå behöver för att genomföra sin tillsyn. I 5 kap. 5 § brottsdatalagen föreskrivs därför att tillsynsmyndigheten ska ges tillgång till de personuppgifter som behandlas, tillgång till dokumentation om behandlingen av dem och övrig dokumentation som behövs för tillsynen. Motsvarande reglering bör även tas in i Säkerhetspolisens nya lag.

Regeringen uttalar i förarbetena till brottsdatalagen att det normala förfarandet bör vara att tillsynsmyndigheten tar hjälp av personal vid den granskade myndigheten för att få tillgång till behandlade personuppgifter. Tillgång på det sättet ska inte betraktas som en rätt till direktåtkomst. I vissa fall skulle det dock kunna underlätta om tillsynsmyndigheten själv i samband med en inspektion på plats får använda datorer och andra medel som tillsynsobjektet använder. En sådan möjlighet torde dock förutsätta att tillsynsmyndigheten ges direktåtkomst till de behöriga myndigheternas information. Tillsynsmyndigheten bör därför ges tillgång till utrustning och andra medel som har anknytning till behandlingen av personuppgifter enbart med hjälp av tillsynsobjektets personal (prop. 2017/18:232 s. 291). Motsvarande bör gälla vid tillsynen över Säkerhetshetspolisens personuppgiftsbehandling.

Tillsynsmyndigheten kan även behöva tillgång till lokaler, utrustning och andra medel som används för att behandla personuppgifter. En sådan bestämmelse finns i brottsdatalagen och bör vara densamma vid tillsynen över Säkerhetspolisens personuppgiftbehandling. Tillsynsmyndigheten bör inte ha rätt att med tvång skaffa sig tillgång till lokaler (jfr Integritet, Offentlighet, Informationsteknik, SOU 1997:39, s. 443 och Personuppgiftslag, prop. 1997/98:44, s. 102). Att göra lokaler tillgängliga ingår dock i den personuppgiftsansvariges samarbetsskyldighet i förhållande till tillsynsmyndigheten (avsnitt 13.2.6).

I 5 kap. 5 § 4 brottsdatalagen föreskrivs att tillsynsmyndigheten har rätt att av den personuppgiftsansvariga på begäran få den hjälp och information som behövs för tillsynen. Sådant biträde kan bestå i att den granskade myndigheten gör lokaler, arkiv och databaser tillgängliga för tillsynsmyndigheten. En förutsättning för att få tillgång till de personuppgifter som behandlas är att personal från Säkerhetspolisen bistår vid tillsynen genom att utföra de sökningar som behövs. Enligt regeringens uppfattning har tillsynsmyndigheten, på motsvarande sätt som i brottsdatalagen, behov av den typen av hjälp och en bestämmelse om det bör tas in i den nya lagen. Bestämmelsen bör utformas som motsvarande bestämmelse i brottsdatalagen. Vid sökningar som görs på direkt begäran av tillsynsmyndigheten bör Säkerhetspolisen inte vara bunden av de begränsningar i fråga om behandlingen av personuppgifter som annars gäller i verksamheten. Det kan t.ex. gälla ändamålen för behandlingen eller hur känsliga personuppgifter får behandlas.

Regeringen återkommer till frågan om vad tillsynsmyndigheten kan göra om Säkerhetspolisen eller personuppgiftsbiträdet inte uppfyller sina skyldigheter (avsnitt 15.5.4).

15.5.2 Både förebyggande och korrigerande befogenheter behövs

Regeringens bedömning: Tillsynsmyndigheten bör ha både förebyggande och korrigerande befogenheter.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning

Tydligare reglering av tillsynsmyndighetens befogenheter

I artikel 47.2 dataskyddsdirektivet görs tydlig skillnad mellan förebyggande och korrigerande befogenheter. Detta återspeglas i regleringen i brottsdatalagen genom att tillsynsmyndighetens befogenheter i förebyggande respektive korrigerande syfte regleras i olika paragrafer som också speglar i vilken ordning befogenheterna ska användas. Det finns inga motsvarande krav när det gäller tillsyn över personuppgiftsbehandling som rör nationell säkerhet. Enligt utredningen är det dock lämpligt att tillsynsmyndigheten får befogenheter som ger möjlighet att successivt använda kraftfullare medel och därigenom stegra påtryckningarna om Säkerhetspolisen inte självmant rättar sig efter tillsynsmyndighetens anvisningar. Regeringen delar den bedömningen. Det innebär att tillsynsmyndigheten bör ha både förebyggande och korrigerande befogenheter. Det bör vidare göras tydlig skillnad mellan de förebyggande och de korrigerande befogenheterna på samma sätt som i brottsdatalagen. Mot bakgrund av Säkerhetspolisens speciella verksamhet är det dock inte självklart att tillsynsmyndigheten bör ha alla de befogenheter som regleras i brottsdatalagen.

15.5.3 Förebyggande befogenheter

Regeringens förslag: Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

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

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: *Datainspektionen* anser att varningar bör vara rättsligt bindande. Övriga remissinstanser yttrar sig inte i denna del.

Skälen för regeringens förslag

Råd och stöd

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning ska den enligt 5 kap. 6 § första stycket brottsdatalagen genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken. Som nyss sagts bör tillsynsmyndigheten ha förebyggande befogenheter. En bestämmelse som motsvarar 5 kap. 6 § första stycket brottsdatalagen bör därför tas in i Säkerhetspolisens datalag.

På vilket sätt förändringen ska åstadkommas bör i första hand lämnas åt Säkerhetspolisen eller personuppgiftsbiträdet att avgöra. I många fall torde det vara tillräckligt att tillsynsmyndigheten upplyser om på vilket sätt personuppgiftsbehandlingen riskerar att strida mot regelverket. Tillsynsmyndigheten är skyldig att lämna skriftliga råd vid förhandssamråd (avsnitt 13.2.5 och 15.4.2).

Varning

Enligt 5 kap. 6 § andra stycket brottsdatalagen får tillsynsmyndigheten utfärda varning i vissa fall. En varning är inte bindande utan är tänkt att kunna användas som ett påtryckningsmedel innan bindande föreläggande att vidta viss åtgärd utfärdas för att i ett enskilt fall markera allvaret. Därigenom kan det förebyggas att behandling som inte är förenlig med regelverket påbörjas. Varning får även användas om en pågående behandling riskerar att strida mot lag eller annan författning.

En varning ska vara skriftlig och tydligt ange på vilket sätt behandlingen riskerar att strida mot regelverket. En varning kan avse vilken form av förändring som helst i behandlingen, t.ex. vilka personuppgifter som får behandlas, hur ett behandlingsystem bör utformas, vilka säkerhetsåtgärder som krävs eller något annat som har betydelse för behandlingen. I förarbetena till brottsdatalagen ansåg regeringen att en varning inte ska vara bindande (prop. 2017/18:232 s. 295). Regeringen gör ingen annan bedömning nu.

Möjligheten att utfärda varning är ny. En varning är ett lämpligt komplement till de förebyggande åtgärder som finns i dag. En bestämmelse som motsvarar 5 kap. 6 § andra stycket brottsdatalagen bör därför tas in i Säkerhetspolisens datalag.

15.5.4 Korrigerande befogenheter

Regeringens förslag: Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att Säkerhetspolisen eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom förebyggande åtgärder försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,

2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller

3. förbjuda fortsatt behandling om bristen är allvarlig.

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

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Vilka åtgärder kan komma i fråga?

Om tillsynsmyndigheten konstaterar att Säkerhetspolisen eller personuppgiftsbiträdet inte uppfyller kraven på författningsenlig personuppgiftsbehandling bör det finnas möjlighet för myndigheten att uppmana Säkerhetspolisen och biträdet att uppfylla sina skyldigheter. Det kan göras genom vissa av de åtgärder som normalt används i det förebyggande arbetet, nämligen råd, rekommendationer eller påpekanden. Om Säkerhetspolisen eller personuppgiftsbiträdet vidtar de åtgärder som krävs så snart tillsynsmyndigheten väcker en sådan fråga, torde det räcka med fortsatt dialog. Tillsynsmyndigheten behöver emellertid också kunna tvinga myndigheten eller personuppgiftsbiträdet att fullgöra sina skyldigheter. Medlen för det är i brottsdatalagen bindande förelägganden, förbud mot fortsatt behandling och beslut om sanktionsavgift.

Som framgår av avsnitt 16.2 bör sanktionsavgift inte kunna tas ut av Säkerhetspolisen. I övrigt bör tillsynsmyndigheten få samma korrigerande befogenheter som enligt brottsdatalagen.

Regleringen bör byggas upp på samma sätt som i brottsdatalagen, vilket innebär att åtgärderna i princip ska prövas i den ordning de anges i bestämmelsen. Det bör dock inte krävas att alla lindrigare åtgärder har beslutats. Om omständigheterna är sådana att det redan från början står klart att fortsatt behandling ska förbjudas, bör tillsynsmyndigheten kunna besluta om det utan att ha prövat någon annan åtgärd först.

Bindande förelägganden

I 5 kap. 7 § brottsdatalagen föreskrivs att tillsynsmyndigheten får förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig. Regleringen innebär att tillsynsmyndigheten kan utfärda bindande beslut som uppmanar tillsynsobjektet att vidta vissa åtgärder för att göra personuppgiftsbehandlingen författningsenlig. Rättelse, radering och begränsning av behandlingen är exempel på åtgärder som tillsynsmyndigheten kan förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta. En motsvarande möjlighet att anta bindande förelägganden bör även gälla för tillsynsmyndigheten i den nya lagen.

När det gäller åtgärder för att göra personuppgiftsbehandlingen författningsenlig kan det i vissa fall vara lämpligt att tillsynsmyndigheten i föreläggandet anger vilken åtgärd som ska vidtas. I många andra fall är

dock Säkerhetspolisen bättre lämpad att avgöra vad som bör göras för att behandlingen ska bli författningsenlig. Det kan t.ex. vara fråga om vilka tekniska åtgärder som bör vidtas eller vilka säkerhetslösningar som bör väljas. Tillsynsmyndigheten bör därför endast om det är lämpligt ange vilken åtgärd som ska vidtas. Däremot ska det alltid framgå när åtgärden ska vara genomförd.

Tillsynsmyndigheten bör även kunna förelägga Säkerhetspolisen att radera uppgiften (jfr prop. 2017/18:232 s. 297). Som framgår av avsnitt 14.4.2 kan radering sällan komma i fråga med hänsyn till reglerna i 2 kap. tryckfrihetsförordningen. Om tillsynsmyndigheten överväger att förelägga tillsynsobjektet att radera uppgiften måste myndigheten beakta att åtgärden inte får stå i strid med annan lagstiftning.

Förelägganden bör inte bara kunna utfärdas för att säkerställa att personuppgiftsbehandling ska vara författningsenlig. För att tillsynsmyndigheten ska ha effektiva befogenheter behöver den även kunna utfärda bindande förelägganden som tar sikte på att Säkerhetspolisen och personuppgiftsbiträden ska uppfylla andra skyldigheter. Det kan t.ex. vara att införa bättre säkerhetslösningar, fullgöra dokumentationsskyldighet eller att överlämna viss dokumentation eller ge tillträde till lokaler. Motsvarande möjlighet för tillsyns-myndigheten finns i brottsdatalagen.

Förbud mot fortsatt behandling

Med förbud mot fortsatt behandling avses att någon behandling inte längre får förekomma. Personuppgifter får dock alltid behandlas om det är nödvändigt med hänsyn till reglerna i 2 kap. tryckfrihetsförordningen.

I 5 kap. 7 § brottsdatalagen finns en bestämmelse om förbud mot fortsatt behandling. En motsvarande bestämmelse bör tas in i Säkerhetspolisens nya datalag. I flera lagstiftningsärenden har det ansetts naturligt att förbud mot fortsatt behandling även bör kunna riktas mot myndigheter (prop. 2009/10:85 s. 275 och Domstolsdatalag, prop. 2014/15:148, s. 89). Åtgärden bör dock på samma sätt som i dag användas restriktivt (jfr prop. 1997/98:44 s. 103). Förbud mot fortsatt behandling bör bara kunna meddelas om en myndighet på ett allvarligt sätt har åsidosatt sina skyldigheter och bristerna är sådana att de inte kan åtgärdas på annat sätt än att behandlingen upphör (jfr Myndighetsdatalag, SOU 2015:39, s. 626 f.).

Att en personuppgift har behandlats på ett sådant sätt att förbud mot fortsatt behandling aktualiseras behöver inte innebära att all behandling av uppgiften måste upphöra. Förbudet måste kopplas till vad som föranledde åtgärden (jfr avsnitt 14.4.3). Hur omfattande förbudet blir beror på vilken typ av personuppgift det är och hur den har behandlats.

Ett förbud mot fortsatt behandling bör normalt vara permanent. I vissa fall kan dock ett tillfälligt förbud vara en lämplig åtgärd, t.ex. om Säkerhetspolisen trots påpekande eller varning från tillsynsmyndigheten har påbörjat otillåten personuppgiftsbehandling och myndigheten bedömer att bristerna kan rättas till.

15.6 Handläggningen av tillsynsfrågor

15.6.1 Förvaltningslagens tillämplighet

På samma sätt som i dag ska förvaltningslagen (2017:900) tillämpas i tillsynsmyndighetens verksamhet. Lagen innehåller grundläggande regler om handläggning av ärenden hos förvaltningsmyndigheterna, men gäller bara i den utsträckning det inte finns avvikande regler i andra författningar. Som tidigare nämnts saknas generell författningsreglering av tillsynsverksamhet. Det är i huvudsak inte heller fråga om ärendehantering utan en arbetsuppgift som kan lösas på olika sätt. I vissa fall lägger dock tillsynsmyndigheten upp ett tillsynsärende för att kunna hantera inkommande handlingar.

15.6.2 Kommunikationsskyldighet

Regeringens bedömning: Det bör inte införas en bestämmelse om kommunikationsskyldighet i lagen.

Utredningens förslag: Utredningen föreslår att en särskild bestämmelse om kommunikation införs.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Utredningen föreslår att det i Säkerhetspolisens nya lag ska införas en bestämmelse om kommunikation inför beslut som tillsynsmyndigheten avser att fatta med stöd av sina korrigerande tillsynsbefogenheter. Av 25 § förvaltningslagen framgår dock att innan en myndighet fattar ett beslut i ett ärende ska den, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Denna bestämmelse fyller samma funktion som utredningens förslag (jfr prop. 2017/18:232 s. 298). Mot denna bakgrund bedömer regeringen att det inte finns något behov av en bestämmelse om kommunikation.

15.6.3 Beslut ska gälla när de fått laga kraft

Regeringens förslag: Tillsynsmyndighetens beslut ska inte få verkställas omedelbart.

Utredningens förslag: Utredningen lämnar inte något förslag i denna del.

Remissinstanserna yttrar sig inte särskilt om detta.

Skälen för regeringens förslag: Enligt 51 § andra stycket personuppgiftslagen får tillsynsmyndigheten besluta att ett av myndigheten meddelat beslut ska gälla även om det överklagas. I polisdatalagen finns dock ingen hänvisning till den bestämmelsen, varför tillsynsmyndigheten i dag inte har möjlighet att fatta interimistiska beslut i förhållande till Säkerhetspolisen.

Som konstaterats i avsnitt 15.6.1 ska tillsynsmyndigheten tillämpa förvaltningslagen i sin verksamhet. I 35 § förvaltningslagen föreskrivs när

beslut får verkställas. Att ett beslut har fått laga kraft är som huvudregel förutsättning för verkställighet. Bestämmelsen innehåller emellertid i andra och tredje styckena vissa undantagssituationer då beslut får verkställas omedelbart. För att tillsynsmyndigheten inte ska kunna besluta att myndighetens beslut ska gälla direkt, behöver detta regleras. Det finns därför anledning att ta in en bestämmelse i den nya lagen om att tillsynsmyndighetens beslut, på samma sätt som i dag, inte ska få verkställas omedelbart. Bestämmelsen bör utformas som motsvarande bestämmelse i brottsdatalagen.

15.7 Säkerhets- och integritetsskyddsnämndens tillsyn

Regeringens förslag: Av lagen om tillsyn över viss brottsbekämpande verksamhet ska det framgå att nämnden ska utöva tillsyn över den personuppgiftsbehandling som Säkerhetspolisen utför.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att tillsynsområdet inte knyts till en uppräkning av författningar. Utredningen lämnar vidare förslag om att nämnden ska ha rätt till de uppgifter, upplysningar och information som den behöver för sin tillsyn och att nämnden ska kunna vägra att utföra kontroll på begäran av enskild om begäran är orimlig eller uppenbart ogrundad.

Remissinstanserna: Både *Säkerhets- och Integritetsskyddsnämnden* och *Datainspektionen* anför att det bör klargöras om det är nämnden eller inspektionen som ska utföra en kontroll på begäran av en enskild i de fall där Polismyndigheten har övertagit en uppgift som rör nationell säkerhet från Säkerhetspolisen.

Skälen för regeringens förslag: Som framgår av avsnitt 15.1.1 utövar nämnden i dag tillsyn över den behandling av personuppgifter som utförs av Säkerhetspolisen enligt polisdatalagen. Regeringen har också beslutat att nämnden ska fortsätta att utöva tillsyn över Polismyndighetens personuppgiftsbehandling (avsnitt 15.1.2). Lagen om tillsyn över viss brottsbekämpande verksamhet har därför ändrats för att anpassas till brottsdatalagen och polisens brottsdatalag (prop. 2017/18:269 s. 280 f.). Eftersom nämnden även fortsättningsvis ska utöva tillsyn över Säkerhetspolisen (avsnitt 15.2) måste den aktuella lagen ändras när Säkerhetspolisens datalag träder i kraft. Ändringen bör utformas på motsvarande sätt som den ändring som gjordes när brottsdatalagen och polisens brottsdatalag trädde i kraft (prop. 2017/18:269 s. 281). Övriga författningsändringar som utredningen föreslår har omhändertagits i nämnda proposition (prop. 2017/18:269 s. 280–282).

Nämnden har i september 2018 inkommit med en framställning om vissa ändringar i lagen om tillsyn över viss brottsbekämpande verksamhet (Ju2018/04361/Å). Det finns inte möjlighet att inom ramen för detta lagstiftningsprojekt behandla framställan.

Eftersom det inte föreslås att det införs bestämmelser om kontroll på begäran av enskild i Säkerhetspolisens nya datalag och då en sådan bestämmelse endast finns i lagen om tillsyn över viss brottsbekämpande

verksamhet, bör nämnden vara den myndighet som utför en kontroll på begäran av en enskild i de fall där Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

16 Sanktioner, skadestånd och rättsmedel

16.1 Ingen straffbestämmelse i den nya lagen

Regeringens bedömning: Överträdelser av bestämmelserna om personuppgiftsbehandling bör inte vara straffsanktionerade utöver vad som gäller enligt brottsbalken.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning: Straffrättsligt ansvar enligt brottsbalken kan utkrävas för vissa gärningar som innefattar otillåten hantering av personuppgifter, t.ex. olaga integritetsintrång enligt 4 kap. 6 § c, dataintrång enligt 4 kap. 9 c § och tjänstefel enligt 20 kap. 1 §. Mot den bakgrunden gällde den bestämmelse om straffansvar vid felaktig personuppgiftsbehandling som fanns i 49 § personuppgiftslagen (1998:204) inte i Säkerhetspolisens verksamhet (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 91).

I lagen (1994:260) om offentlig anställning finns bestämmelser om disciplinansvar som kan aktualiseras om någon bryter mot bestämmelserna om personuppgiftsbehandling. Disciplinansvar förutsätter att den misstänkta gärningen inte ska anmälas till åtal eller, om den redan prövats straffrättsligt, att den inte har ansetts vara något brott av annat skäl än bristande bevisning.

Varken i brottsdatalagen (2018:1177) eller i dataskyddslagen finns det någon straffbestämmelse. I förarbetena till brottsdatalagen uttalas att en kriminalisering motsvarande den som tidigare fanns i 49 § personuppgiftslagen inte skulle vara en lämplig sanktion, eftersom den i huvudsak skulle träffa andra än personuppgiftsansvariga och personuppgiftsbiträden. Straffansvaret skulle i första hand träffa den som faktiskt felbehandlat personuppgifterna, vilket i de flesta fall torde vara en person i underordnad ställning som kanske av oförstånd eller okunskap inte följt reglerna om personuppgiftsbehandling. Överträdelser kan dessutom vara resultatet av flera personers agerande och underlåtenhet. Enligt regeringen blir det då svårt att visa var skulden ligger och vad som lett till överträdelsen. Man valde därför en annan sanktionsform som skulle träffa den personuppgiftsansvarige (Brottsdatalag, prop. 2017/18:232, s. 312).

De skäl mot en straffbestämmelse som framförs i förarbetena till brottsdatalagen gör sig gällande även för Säkerhetspolisen. Mot den bakgrunden och då Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen inte är straffsanktionerad och det inte heller finns någon straffbestämmelse i dataskyddslagen, bör någon sådan bestämmelse inte tas in i den nya lagen.

16.2 Sanktionsavgift bör inte få tas ut

Regeringens bedömning: Det bör inte tas in bestämmelser om sanktionsavgift i den nya lagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast *Datainspektionen* yttrar sig i denna del och anför att skälen för ett enhetligt sanktionssystem är så starka att en bestämmelse om sanktionsavgift bör tas in i den nya lagen.

Skäl för regeringens bedömning

Nuvarande reglering

I 44 och 45 §§ personuppgiftslagen finns bestämmelser som ger tillsynsmyndigheten rätt att vid vite förbjuda behandling på annat sätt än genom lagring. Vidare får tillsynsmyndigheten enligt 47 § hos domstol ansöka om att personuppgifter som behandlats på olagligt sätt ska utplånas. Regleringen i 44, 45 och 47 §§ gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 11 och 6 kap. 4 § polisdatalagen (2010:361). Av 2 kap. 2 § fjärde stycket polisdatalagen framgår emellertid att förbud enligt 44 eller 45 § personuppgiftslagen inte får förenas med vite. I förarbetena motiveras undantaget med att vite inte bör användas mellan statliga myndigheter (prop. 2009/10:85 s. 90).

Ett nytt sanktionssystem i brottsdatalagen

I brottsdatalagen finns bestämmelser om en ny administrativ sanktion – sanktionsavgift. Enligt 6 kap. 1 och 2 §§ får en sanktionsavgift tas ut av en personuppgiftsansvarig och ett personuppgiftsbiträde vid överträdelser av vissa bestämmelser i lagen. Ansvaret är strikt, vilket innebär att det varken krävs uppsåt eller oaktsamhet för att sanktionsavgiften ska kunna tas ut. Enligt 6 kap. 6 § är det tillsynsmyndigheten som fattar beslut om sanktionsavgift. Även registerförfattningarna föreskriver att en sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelser av vissa bestämmelser i lagarna (se exempelvis 7 kap. 1 § polisens brottsdatalag).

Sanktionsavgift bör inte kunna tas ut av Säkerhetspolisen

Frågan är om det bör införas ett sanktionssystem som motsvarar det i brottsdatalagen även för Säkerhetspolisen. Säkerhetspolisen ska tillämpa brottsdatalagen och polisens brottsdatalag i vissa fall (avsnitt 7.5). Myndigheten kommer då att omfattas av sanktionssystemet i de lagarna. Även dataskyddsförordningen föreskriver att administrativa sanktionsavgifter ska kunna tas ut vid överträdelse av bestämmelser om personuppgiftsbehandling.

Huvudskälet till att regeringen föreslog att sanktionsavgift skulle kunna tas ut av behöriga myndigheter i brottsdatalagen var att motsvarande sanktionssystem gäller enligt dataskyddsförordningen. Eftersom de behöriga myndigheterna tillämpar båda regelverken finns det fördelar med en enhetlig reglering. För flera av myndigheterna regleras också en större del av personuppgiftsbehandlingen av dataskyddsförordningen. Det gäller

Skatteverket, Tullverket och domstolarna. Även Polismyndigheten tillämpar dataskyddsförordningen. Det blev då svårt att motivera att helt olika sanktionssystem skulle gälla beroende på om brottsdatalagen eller förordningen är tillämplig vid överträdelser som är likartade och som därför kan antas motivera samma sanktion (prop. 2017/18:232 s. 311–317).

Säkerhetspolisen kommer att tillämpa dataskyddsförordningen i en begränsad del av verksamheten som är av intern och administrativ karaktär. Det är också bara i speciella fall som myndigheten kommer att tillämpa brottsdatalagen och polisens brottsdatalag. Skälen för ett enhetligt sanktionssystem gör sig därför inte gällande på samma sätt i Säkerhetspolisens verksamhet. Eftersom Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av dataskyddsdirektivets eller dataskyddsförordningens tillämpningsområde är regeringen inte heller bunden av de krav på sanktioner som ställs i dessa rättsakter.

Dataskyddskonventionen, som även omfattar personuppgiftsbehandling som rör nationell säkerhet (avsnitt 5.1), ställer krav på att det ska finnas lämpliga sanktioner för överträdelser av bestämmelser om dataskydd. I konventionen anges dock inte vilka krav som ställs på sådana sanktioner. Regeringen delar utredningens bedömning att konventionens krav på sanktioner inte är lika långtgående som dataskyddsdirektivets och dataskyddsförordningens krav. Den nuvarande regleringen ger möjlighet till ersättning genom skadestånd. Vidare kan straffrättsligt ansvar utkrävas enligt brottsbalken.

I avsnitt 16.3.2 föreslår regeringen att Säkerhetspolisen ska kunna åläggas skadestånd vid felaktig personuppgiftsbehandling. I avsnitt 15 diskuteras hur tillsynen över Säkerhetspolisens personuppgiftsbehandling bör utövas och vilka befogenheter tillsynsmyndigheten bör ha. Sanktionssystemet i den nya lagen kommer att motsvara det som gäller i dag.

Sammanfattningsvis anser regeringen i likhet med utredningen att de sanktionsmöjligheter som finns i dag är tillräckliga. Eftersom skälen för ett enhetligt sanktionssystem inte heller har samma styrka när det gäller behandling av personuppgifter som rör nationell säkerhet, anser regeringen, till skillnad från *Datainspektionen*, att det inte bör införas någon möjlighet att ta ut sanktionsavgift vid överträdelse av bestämmelser i den nya lagen.

16.3 Skadestånd

16.3.1 Det allmännas skadeståndsansvar

Enligt 3 kap. 2 § skadeståndslagen (1972:207) ska staten eller en kommun ersätta personskada, sakskada eller ren förmögenhetsskada som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommunen svarar. Ersättningsskyldigheten omfattar även ideell skada på grund av att någon genom fel eller försummelse vid myndighetsutövning kränkts på det sätt som anges i 2 kap. 3 § samma lag.

I 2 kap. 3 § skadeståndslagen föreskrivs att den som allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära ska ersätta den skada som kränkningen innebär. Ideellt skadestånd för att den personliga integriteten har kränkts, dvs. en skada av icke-ekonomisk natur, förutsätter alltså att kränkningen har orsakats genom brott. Det krävs också att kränkningen är allvarlig.

Ersättning för kränkning med stöd av 3 kap. 2 § jämförd med 2 kap. 3 § skadeståndslagen förutsätter att kränkningen har orsakats vid myndighetsutövning. Om det inte är fråga om myndighetsutövning kan skadestånd ändå utgå enligt 3 kap. 1 § skadeståndslagen för skada som vållats av arbetstagare. Det förutsätter att kränkningen har orsakats av att den anställde har begått brott i tjänsteutövningen.

Genom Högsta domstolens praxis har det lagts fast en rätt till ideellt skadestånd vid kränkningar av Europakonventionen även i andra fall än de som regleras i skadeståndslagen. Det har bl.a. varit fråga om kränkningar av rätten till privat- och familjeliv enligt artikel 8 i konventionen. En ny bestämmelse i skadeståndslagen om rätten till skadestånd vid överträdelser enligt Europakonventionen trädde i kraft den 1 april 2018 (Skadestånd och Europakonventionen, prop. 2017/18:7).

Den som anser att han eller hon har orsakats skada av det allmänna kan väcka talan mot staten eller en kommun vid allmän domstol. Saken prövas då som tvistemål.

Enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten kan en skadelidande dessutom få ett skadeståndskrav mot staten prövat inom ramen för statens frivilliga skadereglering. Med det avses skadereglering som företrädelsevis sker hos Justitiekanslern, men som även i viss omfattning kan förekomma hos andra myndigheter. Enligt förordningen kan den enskilde i ett formlöst och kostnadsfritt förfarande vända sig direkt till en myndighet och få ett besked i frågan om huruvida staten är skadeståndsskyldig. Det är ett särskilt snabbt och effektivt sätt att komma i åtnjutande av det rättsmedel som rätten till skadestånd innebär. Vid ett negativt besked har den enskilde kvar möjligheten att vända sig till domstol för att få saken prövad. Justitiekanslerns inställning är inte bindande för domstolarna eller för den enskilde. Enligt förordningen kan Justitiekanslern bl.a. handlägga anspråk som grundas på 3 kap. 1 eller 2 § skadeståndslagen eller skadeståndsregler i vissa särskilt angivna författningar, t.ex. 7 kap. 1 § brottsdatalagen.

16.3.2 Skadeståndsskyldighet för den personuppgiftsansvarige

Regeringens förslag: Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med den nya lagen eller föreskrifter som meddelats i anslutning till den.

Regeringens bedömning: Det bör inte införas någon jämkningsregel i lagen.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: *Justitiekanslern* välkomnar den föreslagna hänvisningen till Säkerhetspolisens nya lag i 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten. *Sveriges advokatsamfund* ställer sig tveksam till om möjligheten till skadestånd kommer att få någon praktisk effekt på grund av svårigheten att driva en sådan talan.

Skälen för regeringens förslag och bedömning

Nuvarande reglering

Enligt 48 § första stycket personuppgiftslagen ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med lagen har orsakat. Alla åtgärder som är oförenliga med personuppgiftslagen kan leda till skadeståndsskyldighet, om de allmänna kraven för skadestånd är uppfyllda. Ersättningsskyldighet inträder så snart en bestämmelse överträtts, vilket gör att skadeståndsansvaret är strikt. Enligt 48 § andra stycket kan ersättningsskyldigheten, om det är skäligt, jämkas om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Bestämmelsen i 48 § personuppgiftslagen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 12 och 6 kap. 4 § 1 polisdatalagen.

I 7 kap. 1 § brottsdatalagen finns en bestämmelse som motsvarar 48 § första stycket personuppgiftslagen. Eftersom det inte finns någon exculperingsbestämmelse i direktivet har regeringen inte ansett det möjligt att öppna för möjlighet till jämkning i brottsdatalagen (prop. 2017/18:232 s. 344.).

Det bör införas en regel om skadeståndsskyldighet i den nya lagen

Det bör i den nya lagen finnas en bestämmelse som reglerar den personuppgiftsansvariges dvs. Säkerhetspolisens och Polismyndighetens skadeståndsansvar. Den bör formuleras på samma sätt som i brottsdatalagen. Den synpunkt som *Sveriges advokatsamfund* har lämnat i fråga om möjligheterna att driva en skadeståndstalan föranleder inte någon annan bedömning.

Bestämmelsen skulle kunna föreskriva att skadeståndsersättning får jämkas, eftersom regleringen inte behöver följa direktivets bestämmelser. Det underlättar emellertid både för tillämparen och för den enskilde om regleringen i den delen stämmer överens med övriga registerförfattningar på området. Intresset av en enhetlig reglering väger enligt regeringen tyngre än den personuppgiftsansvariges intresse av att eventuella skadeståndsanspråk i vissa fall kan jämkas. Den nya lagen bör därför inte innehålla någon jämkningsbestämmelse.

Enligt 48 § personuppgiftslagen är det enbart den personuppgiftsansvarige som är skadeståndsskyldig. Gentemot den registrerade är den personuppgiftsansvarige ansvarig för all behandling, dvs. även när ett personuppgiftsbiträde eller annan hjälp anlitas. Om fel har begåtts av t.ex. ett personuppgiftsbiträde anses det alltså bero på den personuppgiftsansvarige.

Enligt dataskyddsförordningen ska det även finnas möjlighet att rikta skadeståndstalan mot personuppgiftsbiträden (artikel 82.1), men i dataskyddsdirektivet finns ingen motsvarande bestämmelse. Enligt brottsdatalagen är det därför bara den personuppgiftsansvarige som är skadeståndsansvarig. För den registrerade tillgodoses rätten till ersättning för skada som ett personuppgiftsbiträde har orsakat genom att den personuppgiftsansvarige är ansvarig även för biträdets handlande. Det finns inte skäl att frångå denna ordning i den nya lagen.

Det finns dock skäl att erinra om att ett personuppgiftsbiträde ibland är att anse som personuppgiftsansvarig för viss behandling och då givetvis kan bli skadeståndsskyldig i den egenskapen (avsnitt 13.4.4).

I dag prövar Justitiekanslern frågor om skadeståndsskyldighet enligt 48 § personuppgiftslagen. Frågan om myndigheten bör pröva om staten är skadeståndsskyldig enligt den nya lagen tas om hand i samband med framtagandet av förordningsändringar.

Skadeståndets omfattning

Rätten till personlig integritet är en immateriell rättighet. Den personuppgiftsansvarige är därför ersättningsskyldig inte bara för ekonomisk skada utan även för ideell skada. Den enskilde har alltså, förutom rätt till ersättning för personskada, sakskada och ren förmögenhetsskada, rätt till ekonomisk kompensation för kränkningen. Det är bara skada eller kränkning som behandlingen har fört med sig som ska ersättas. Orsakssambandet ska vara adekvat.

Som regeringen konstaterar i förarbetena till brottsdatalagen möter den nuvarande skadeståndsregeln i personuppgiftslagen både kravet på att all skada ska ersättas och att det ska finnas adekvat kausalitet. Skadeståndsbestämmelsen i brottsdatalagen har därför utformats med den som mönster (prop. 2017/18:232 s. 343). Detsamma bör gälla för skadeståndsbestämmelsen i den nya lagen. Den bör i huvudsak kunna tolkas i enlighet med den praxis som har utvecklats med anledning av bestämmelsen i personuppgiftslagen.

Hur ska ersättningen för kränkning beräknas?

Liksom i dag bör ersättningen för kränkning uppskattas efter skälighet, mot bakgrund av samtliga omständigheter. Det som kan ha betydelse är bl.a. att personuppgifter spridits eller att det funnits risk för otillbörlig spridning av integritetskänsliga eller felaktiga personuppgifter. En annan omständighet kan vara att den registrerade drabbats av beslut eller andra åtgärder som fått eller kunnat få negativa konsekvenser för honom eller henne. Om den registrerade själv har lämnat oriktig eller ofullständig information till den personuppgiftsansvarige, kan även detta ha betydelse vid beräkningen. En jämförelse kan göras med vad som gäller i fråga om betydelsen av den skadelidandes eget agerande när det gäller kränkningsersättning vid brott (Ersättning för ideell skada, prop. 2000/01:68, s. 52).

Förhållandet till skadeståndslagen

Bestämmelsen i den nya lagen kommer i likhet med 48 § personuppgiftslagen att vara en sådan specialbestämmelse om skadestånd som enligt 1 kap. 1 § skadeståndslagen tar över de allmänna reglerna i den lagen. Om

en ersättningsfråga inte regleras i den nya lagen – t.ex. hur ersättningen för en personskada eller sakskada ska beräknas (5 kap. skadeståndslagen) eller hur ansvaret ska fördelas när flera är skadeståndsskyldiga (6 kap. 4 § skadeståndslagen) – tillämpas de allmänna reglerna i skadeståndslagen.

16.4 Överklagande

16.4.1 Överklagande av den personuppgiftsansvariges beslut

Regeringens förslag: Beslut i fråga om rättelse, komplettering, radering eller begränsning av behandlingen som har meddelats på begäran av den registrerade, ska kunna överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad eller att ta ut avgift för att lämna sådan information. Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Några andra beslut än de som uttryckligen anges i lagen ska inte få överklagas.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Behov av en överklagandebestämmelse i den nya lagen

Enligt 52 § första stycket personuppgiftslagen får vissa beslut som fattas av en personuppgiftsansvarig som är en myndighet överklagas till allmän förvaltningsdomstol. Det gäller beslut om information enligt 26 §, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 13 och 6 kap. 4 § 1 polisdatalagen.

Det är naturligt att se en myndighets beslut i egenskap av personuppgiftsansvarig, exempelvis i fråga om en personuppgift ska rättas eller inte, som ett utflöde av dess myndighetsutövning. I allmänhet har myndigheten behandlat personuppgifterna i syfte att fullgöra myndighetsuppgifter. Personuppgifterna har också normalt behandlats med stöd av olika författningsbestämmelser, oberoende av den registrerades samtycke. I 7 kap. 2 § brottsdatalagen finns därför en bestämmelse som motsvarar 52 § första stycket personuppgiftlagen. En liknande bestämmelse bör, som utredningen föreslår, tas in även i den nya lagen.

Vilka beslut ska kunna överklagas?

När det gäller enskildas rätt att överklaga myndighetsbeslut bör samma utgångspunkt gälla som i fråga om rätten att överklaga beslut enligt personuppgiftslagen. Överklaganderätten bör alltså enbart ta sikte på sådana beslut av myndigheten som den fattat i egenskap av personuppgiftsansvarig och som direkt berör den enskilde och som gått honom eller henne

emot. Sådana beslut bör på samma sätt som andra förvaltningsbeslut kunna överklagas till allmän förvaltningsdomstol.

Enligt 7 kap. 2 § brottsdatalagen kan beslut som fattas på begäran av en registrerad om att personuppgifter ska rättas, kompletteras eller raderas eller att behandlingen av personuppgifter ska begränsas överklagas. Det gäller oavsett om myndigheten avslår begäran eller vidtar en annan åtgärd än den som begärts. Har myndigheten helt eller delvis underlåtit att lämna information som den enskilde har begärt, kan beslutet överklagas. Även beslut att ta ut avgift för information eller att vägra omprövning av ett automatiserat beslut kan överklagas. Uppräkningen motsvarar i allt väsentligt de beslut som i dag får överklagas enligt 52 § personuppgiftslagen. På samma sätt som i brottsdatalagen bör det i den nya lagen framgå vilka beslut som får överklagas. Eftersom det inte förekommer några automatiserade beslut i Säkerhetspolisens verksamhet behövs dock inte någon bestämmelse om överklagande av sådana beslut.

Överklagandena bör, på samma sätt som i dag, prövas av allmän förvaltningsdomstol. Vid överklagande till kammarrätten bör det krävas prövningstillstånd.

Vad bör inte få överklagas?

Av 53 § personuppgiftslagen framgår att andra beslut som en personuppgiftsansvarig myndighet fattat enligt lagen inte får överklagas. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 13 och 6 kap. 4 § 1 polisdatalagen.

På samma sätt som i dag bör inte alla beslut som Säkerhetspolisen fattar i egenskap av personuppgiftsansvarig få överklagas. Administrativa beslut av myndigheten, t.ex. i fråga om tillgången till personuppgifter, berör inte den enskilde på ett sådant sätt att de ska få överklagas. Det bör därför av den nya lagen framgå att andra beslut än de som räknas upp inte får överklagas. En motsvarande bestämmelse finns i brottsdatalagen.

16.4.2 Överklagande av tillsynsmyndighetens beslut

Regeringens förslag: Tillsynsmyndighetens beslut enligt den nya lagen ska få överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Utredningens förslag överensstämmer i huvudsak med regeringens. I utredningens förslag anges inte uttryckligen att tillsynsmyndigheten har ställning som motpart i domstolen. Enligt utredningens förslag ska även tillsynsmyndighetens beslut enligt föreskrifter som meddelats i anslutning till lagen få överklagas till allmän förvaltningsdomstol.

Remissinstanserna: *Kammarrätten i Stockholm* och *Förvaltningsrätten i Stockholm* anser att det bör klargöras att tillsynsmyndigheten är motpart om dess beslut överklagas.

Skälen för regeringens förslag

En överklagandebestämmelse bör tas in i den nya lagen

Enligt 42 § förvaltningslagen (2017:900) får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Enligt 51 § första stycket personuppgiftslagen får tillsynsmyndighetens beslut, med undantag av beslut om föreskrifter, överklagas till allmän förvaltningsdomstol. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § första stycket 13 och 6 kap. 4 § 1 polisdatalagen.

Om en myndighets befogenheter regleras i en författning bör det som huvudregel av samma författning framgå om och i så fall hur myndighetens beslut kan överklagas. En sådan ordning ger en samlad bild både av vilka befogenheter en myndighet har och hur den som blir föremål för myndighetens beslut kan angripa dem. Regeringen föreslår nu att tillsynsmyndighetens befogenheter regleras i den nya lagen (avsnitt 15.1.3). Den nya lagen bör därför även reglera rätten att överklaga tillsynsmyndighetens beslut. En motsvarande bestämmelse finns i 7 kap. 4 § brottsdatalagen.

Vilka beslut ska få överklagas?

Rätten att överklaga beslut regleras genom bestämmelser i specialförfattningar och myndighetsinstruktioner. Även om det i en författning anges att ett beslut enligt författningen eller ett beslut av en viss myndighet får överklagas, innebär det inte att alla sådana beslut är överklagbara. Överklagbarheten är nämligen begränsad till följd av allmänna principer som har utbildats i rättspraxis (jfr RÅ 2007 ref. 7 och där angivna rättsfall). En myndighets faktiska handlande eller underlåtenhet att handla kan exempelvis inte överklagas. Normalt saknas det också möjlighet att klaga över motiveringen till ett beslut (prop. 1997/98:101 s. 49 f.). En annan begränsning för överklagande är att beslutet inte får ha en alltför obetydlig verkan för parter eller andra. Frågan om överklagbarhet har prövats när det gäller tillsynsmyndighetens beslut enligt personuppgiftslagen, för exempel se Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen, En kommentar, 4:e uppl. 2011, i fortsättningen Öman m.fl. m.fl. s. 549 f.

Bestämmelsen i den nya lagen bör med beaktande av det som nu har sagts och i likhet med dagens reglering ha som utgångspunkt att tillsynsmyndighetens beslut ska kunna överklagas. Av tydlighetsskäl bör det, som *Kammarrätten i Stockholm* och *Förvaltningsrätten i Stockholm* anför, även framgå av bestämmelsen att tillsynsmyndigheten har ställning som motpart i ett sådant mål hos domstolen (jfr 22 kap. 5 § lagen [2016:1145] om offentlig upphandling). Det kan i vissa fall vara svårt att förutse vilka beslut som går att överklaga. En fullständig reglering är emellertid inte lämplig att göra. På samma sätt som i dag får det i stället avgöras i rättstillämpningen om ett beslut som tillsynsmyndigheten har fattat är överklagbart.

Överklagandena bör på samma sätt som i dag prövas av allmän förvaltningsdomstol. Det bör krävas prövningstillstånd vid överklagande till kammarrätten.

Till skillnad från utredningen ansåg regeringen i förarbetena till brottsdatalagen att överklagandemöjligheten avseende beslut enligt föreskrifter

inte bör regleras i den nya lagen (prop. 2017/18:232 s. 353). Det finns inte skäl att här göra en annan bedömning.

Vem får överklaga?

För att någon ska få överklaga ett beslut ska han eller hon ha klagorätt. Om en person har klagorätt måste bedömas i varje enskilt fall av den domstol som behandlar överklagandet.

I 51 § personuppgiftslagen ställs det inte något krav på att den som klagar ska vara part. I praxis har det inte heller krävts att den som överklagar tillsynsmyndighetens beslut har ställning som part. I stället har det bl.a. förts resonemang kring dels om beslutet angått den som överklagat det, dels om det gått honom eller henne emot. Det finns inte heller skäl att i den nya lagen ställa krav på att den som klagar ska vara part. Bestämmelsen om överklagande av tillsynsmyndighetens beslut bör därför utformas med 51 § första stycket personuppgiftslagen som mönster.

Att det är den som beslutet angår och som det gått emot som har klagorätt innebär i praktiken att det är den beslutet riktas mot som har rätt att överklaga tillsynsmyndighetens beslut. I ett tillsynsärende kommer det oftast att vara Säkerhetspolisen eller ett personuppgiftsbiträde. Det kan dock inte uteslutas att beslut av tillsynsmyndigheten i något annat fall skulle kunna få rättsliga följder även för någon annan än den som beslutet riktar sig mot. Vederbörande har då rätt att överklaga beslutet enligt förvaltningslagens regler om talerätt.

Särskilt om Säkerhetspolisens rätt att överklaga

De allmänna förvaltningsrättsliga principerna om klagorätt anses bara vara tillämpliga på myndigheter när de uppträder i någon privaträttslig egenskap, exempelvis som arbetsgivare eller fastighetsägare. Då anses myndigheter ha samma rätt att överklaga som enskilda. När myndigheter däremot uppträder i sin offentligrättsliga roll, vilket de gör i egenskap av personuppgiftsansvariga, är förhållandena annorlunda. En myndighet får då överklaga en annan myndighets beslut bara under vissa förutsättningar. Utgångspunkten är då att överklagande kräver författningsstöd.

Säkerhetspolisen anses redan i dag kunna överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol enligt 51 § personuppgiftslagen. Detsamma bör gälla enligt den nya lagen.

17 Överföring av personuppgifter till tredjeland och internationella organisationer

17.1 Utgångspunkter

Regeringens förslag: Överföring av personuppgifter till tredjeland och internationella organisationer ska regleras i den nya lagen. Regleringen ska i huvudsak motsvara den som finns i brottsdatalagen.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Nuvarande reglering

I 33–35 §§ personuppgiftslagen (1998:204) finns det bestämmelser om överföring av personuppgifter till tredjeland. De gäller genom hänvisningar i 2 kap. 2 § 8 och 6 kap. 4 § 1 polisdatalagen (2010:361) för Säkerhetspolisen. Enligt 33 § personuppgiftslagen är det förbjudet att till tredjeland föra över personuppgifter som är under behandling, om landet inte har en adekvat skyddsnivå för personuppgifter. Förbudet gäller även överföring av personuppgifter för behandling där. Trots avsaknad av adekvat skyddsnivå är, enligt 34 §, överföring av personuppgifter till tredjeland tillåten om den enskilde har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig i vissa särskilt uppräknade fall. Paragrafen reglerar således vissa undantag från överföringsförbudet i 33 §. Ett viktigt undantag är att personuppgifter får överföras för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Enligt 35 § personuppgiftslagen kan regeringen föreskriva ytterligare undantag från förbudet, bl.a. om det behövs med hänsyn till ett viktigt allmänt intresse.

Regleringen i brottsdatalagen

Överföring av personuppgifter till tredjeland och internationella organisationer regleras i 8 kap. brottsdatalagen (2018:1177). Av 8 kap. 1 § framgår att personuppgifter får överföras till ett tredjeland eller en internationell organisation om överföringen är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Överföringen ska riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet. Personuppgifter får dessutom överföras endast om Europeiska kommissionen (i fortsättningen kommissionen) har antagit beslut om adekvat skyddsnivå, om personuppgifterna omfattas av tillräckliga skyddsåtgärder hos adressaten eller om ett undantag för särskilda situationer är tillämpligt. I 8 kap. 2 § föreskrivs att personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

I 8 kap. 3–5 §§ brottsdatalagen regleras de tillåtna grunderna för överföring närmare. Det finns också bestämmelser om vidareöverföring (6 och 7 §§), om överföring till andra än behöriga myndigheter (8 §) och om användningsbegränsningar (9 och 10 §§).

Överföring av personuppgifter till tredjeland och internationella organisationer ska regleras

Informationsutbyte är en central del av Säkerhetspolisens samarbete med andra stater. Samarbetet berör stater både inom och utanför EU. Som på många andra områden är samarbetet med övriga nordiska länder särskilt nära. I förarbetena till polisdatalagen ansågs att bestämmelserna om

överföring av personuppgifter till tredjeland borde gälla även för Säkerhetspolisen (Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 88 och 252 f.). Den nuvarande regleringen, som är väl inarbetad, är därmed uppbyggd på det sättet.

En reglering som innebär högre krav för överföringar till stater som inte är medlemmar i EU eller anslutna till EES-samarbetet är viktig ur integritetssynpunkt, eftersom det inte kan garanteras samma skydd för personuppgifterna i sådana stater. I 8 kap. brottsdatalagen ställs det högre krav när personuppgifter ska överföras till tredjeland och internationella organisationer. Enligt regeringens mening bör i huvudsak samma krav gälla för Säkerhetspolisen. Det finns därför inte skäl att nu välja en annan lösning beträffande överföring av personuppgifter till tredjeland och internationella organisationer. Villkoren för sådana överföringar bör således regleras i den nya lagen.

Utgångspunkten bör vara att Säkerhetspolisen ska kunna överföra personuppgifter till tredjeland och internationella organisationer i samma utsträckning som i dag. Bestämmelserna i brottsdatalagen bör tas som utgångspunkt. Regleringen av överföringar till tredjeland och internationella organisationer kommer därmed att bli betydligt utförligare men ger samtidigt större möjligheter att överföra personuppgifter till sådana mottagare än i dag.

17.2 Några grundläggande begrepp

Regeringens förslag: Tredjeland ska definieras som en stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning.

Internationell organisation ska definieras som en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Som utredningen föreslår bör tredjeland och internationell organisation definieras i den nya lagen. Definitionerna bör som anges i avsnitt 7.7 så långt möjligt överensstämma med de definitioner som används i brottsdatalagen.

Enligt 1 kap. 6 § brottsdatalagen definieras tredjeland som en stat som inte är en medlemsstat. Medlemsstat definieras som en stat som är medlem i Europeiska unionen samt Island, Liechtenstein, Norge och Schweiz (Brottsdatalag, prop. 2017/18:232, s. 363–365). I den nya lagen kan definitionen av som utgör tredjeland inte på samma sätt som i brottsdatalagen utgå från medlemsstat då detta uttryck inte förekommer i lagen. I stället bör uttrycket stat användas. Med tredjeland bör i lagen avses en stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning. Det innebär att EU:s

medlemsstater, Island, Norge, Liechtenstein och Schweiz inte utgör tredjeland i lagens mening.

I brottsdatalagen avses med en internationell en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater. En motsvarande definition bör tas in i den nya lagen.

17.3 Förutsättningar för överföring

Regeringens förslag: Säkerhetspolisen ska få överföra personuppgifter som behandlas i Sverige till ett tredjeland eller en internationell organisation om överföringen riktas till en brottsbekämpande myndighet, en underrättelse- eller säkerhetstjänst eller en internationell organisation med brottsbekämpande uppdrag. Personuppgifterna får endast överföras om viss skyddsnivå är säkerställd hos mottagaren.

Regleringen ska gälla även vid överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation.

Utredningens förslag: överensstämmer delvis med regeringens. Utredningen förslår att personuppgifter som Säkerhetspolisen har fått från en annan stat ska få överföras till ett tredjeland eller en internationell organisation endast om den stat som lämnat uppgifterna till Säkerhetspolisen har medgett att de överförs.

Remissinstanserna: *Säkerhetspolisen* förordar att bestämmelsen om att överföring av personuppgifter från andra stater ska vara medgiven stryks. Myndigheten anser också att det behöver förtydligas att överföring av personuppgifter från Säkerhetspolisen inte är begränsad till en underrättelse- och säkerhetstjänst med brottsbekämpande uppdrag. *Datainspektionen* och *Sveriges advokatsamfund* efterfrågar en djupare analys av riskerna med att överföra personuppgifter till tredjeland och internationella organisationer.

Skälen för regeringens förslag

De grundläggande förutsättningarna för överföring ska anges

Utgångspunkten i den nya lagen bör, liksom i brottsdatalagen, vara att Säkerhetspolisen ska få överföra personuppgifter till ett tredjeland eller en internationell organisation endast om vissa villkor är uppfyllda. En bestämmelse som anger de grundläggande förutsättningarna för överföring bör tas in i den nya lagen.

Enligt dataskyddsdirektivet får personuppgifter överföras endast om det är nödvändigt för vissa angivna ändamål och överföringen görs till någon som är behörig myndighet. Bestämmelsen i brottsdatalagen har utformats med det som utgångspunkt. Det är inte möjligt att ställa upp samma krav i den nya lagen, bl.a. eftersom regleringen inte bygger på att det är behöriga myndigheter som utbyter uppgifter med varandra. Regleringen i den nya lagen bör därför utformas med brottsdatalagen som mönster, men vissa frågor kräver en annan lösning.

När det gäller Säkerhetspolisen finns det, i motsats till andra brottsbekämpande myndigheter, inte några internationella åtaganden som

innebär en skyldighet att lämna viss information. Säkerhetspolisen råder därmed i större utsträckning över vilken information som lämnas, på vilket sätt det görs och vilka villkor som ställs för den andra statens användning av informationen. Uppgiftsutbyte sker huvudsakligen inom ramen för överenskommelser och bygger på ömsesidigt förtroende. Mot den bakgrunden bör någon motsvarighet till kravet i brottsdatalagen på att överföringen ska vara nödvändig för vissa angivna ändamål inte finnas.

Frågan är om regleringen, på samma sätt som i brottsdatalagen, bör ta sikte på överföring till vissa mottagare. En sådan reglering ger större förutsebarhet och bättre integritetsskydd och bör därför väljas framför en mer generell reglering. I den grundläggande bestämmelsen bör det därför anges att överföringen ska riktas till en brottsbekämpande myndighet, en underrättelse- eller säkerhetstjänst i tredjeland eller till en internationell organisation som har ett brottsbekämpande uppdrag. Det tillgodoser enligt regeringens mening Säkerhetspolisens behov av att kunna överföra personuppgifter i syfte att bistå myndigheter i andra stater. Säkerhetspolisens möjlighet att i vissa fall överföra personuppgifter till andra aktörer behandlas i avsnitt 17.5.

I brottsdatalagen ställs det krav på att vissa skyddsnivåer ska vara säkerställda för att personuppgifter ska få överföras. Personuppgifterna får endast överföras om det finns beslut om adekvat skyddsnivå, om personuppgifterna omfattas av tillräckliga skyddsåtgärder hos adressaten eller om ett undantag för särskilda situationer är tillämpligt. Syftet med regleringen är att den skyddsnivå som säkerställs genom dataskyddsdirektivet och som gäller inom EU som utgångpunkt ska gälla även när personuppgifter överförs till ett tredjeland eller en internationell organisation. Regeringen delar utredningen uppfattning att det är det rimligt att samma krav ställs på Säkerhetspolisen även om myndighetens verksamhet inte omfattas av direktivets tillämpningsområde. Liknande krav på skydd ställs i dag i bl.a. personuppgiftslagen. Den närmare innebörden av dessa krav behandlas i avsnitt 17.4.

Det kan, som *Datainspektionen* och *Sveriges advokatsamfund* påpekar, vara förenat med viss osäkerhet att överföra personuppgifter till ett tredjeland eller en internationell organisation. Det kommer att vila ett stort ansvar på Säkerhetspolisen när det gäller bedömningarna i vilka fall personuppgifter kan överföras. Säkerhetspolisen är dock van vid att göra denna typ av bedömningar. I sammanhanget bör också nämnas att förslaget i denna del ansluter nära till vad som gäller enligt befintlig lagstiftning. Underrättelsearbetet bygger vidare, som tidigare har nämnts, på ett ömsesidigt förtroende. En motpart som missbrukar förtroendet kommer inte längre att få del av information. Här bör också anmärkas att Säkerhetspolisen naturligtvis aldrig är skyldig att överföra personuppgifter till ett tredjeland eller en internationell organisation.

Ingen reglering om att överföring av uppgifter till andra stater ska vara medgiven

I 8 kap. 2 § brottsdatalagen föreskrivs att en överföring av personuppgifter som härrör från en annan medlemsstat ska vara medgiven. Något sådant krav gäller inte för Säkerhetspolisen i dag. Utredningen föreslår att det införs en sådan bestämmelse i den nya lagen.

För att skydda underrättelseinformation tillämpar Säkerhetspolisen den s.k. tredjepartsregel. Regeln, som tillämpas både i det internationella och nationella samarbetet, innebär att uppgifter som myndigheten har fått från en samarbetspartner inte får föras vidare utan uttryckligt samtycke. Regeln är central i Säkerhetspolisens verksamhet och utgör grunden för ett effektivt underrättelseutbyte. Den har tillkommit i syfte att skapa förtroende mellan bl.a. underrättelse- och säkerhetstjänsterna, eftersom det finns ett stort behov av att skydda uppgifter om bl.a. källor och arbetsmetoder.

Säkerhetspolisen har ifrågasatt behovet av att reglera tredjepartsregeln i lag och anfört att den är självreglerande, eftersom en underrättelse- och säkerhetstjänst som bryter mot regeln inte längre åtnjuter det förtroende som krävs för att få del av relevant information. Därutöver anser myndigheten att den föreslagna bestämmelsen inte till fullo överensstämmer med regeln.

Som framgår ovan tillämpar Säkerhetspolisen den aktuella regeln inte bara i förhållande till underrättelse- och säkerhetstjänster i tredjeland utan även i förhållande till andra samarbetspartners. Att lagstadga regeln endast i förhållande till underrättelse- och säkerhetstjänster i tredjeland är inte lämpligt, eftersom det då kommer att råda osäkerhet om vad som gäller i förhållande till andra samarbetsparter. Mot den bakgrunden anser regeringen att det inte bör regleras att information som Säkerhetspolisen fått från en stat inte får överföras till en annan stat utan medgivande från den stat som lämnat informationen.

17.4 Viss skyddsnivå ska vara säkerställd

17.4.1 Beslut om adekvat skyddsnivå

Regeringens förslag: Om kommissionen har beslutat att det finns adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt 8 kap. 3 § brottsdatalagen får personuppgifter överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att landet eller organisationen säkerställer en adekvat nivå för skyddet av personuppgifter. Detsamma gäller om kommissionen har beslutat att det finns en adekvat skyddsnivå i en viss geografisk eller på annat sätt angiven del av ett tredjeland. Ett sådant beslut skulle kunna avse t.ex. en region eller en viss myndighet i ett tredjeland. Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation ska också vara uppfyllda för att personuppgifter ska få överföras. Det motsvarar vad som tidigare gällde enligt 13 § första stycket 1 personuppgiftsförordningen. Även om Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av unionsrätten bör kommissionens beslut om adekvat skyddsnivå, som

utredningen föreslår, vara vägledande för myndigheten. Finns det inget beslut om adekvat skyddsnivå får Säkerhetspolisen i stället pröva om det finns tillräckliga skyddsåtgärder eller om det är fråga om en sådan undantagssituation att överföring ändå får göras. Att kommissionen har återkallat ett beslut om adekvat skyddsnivå bör likställas med att det saknas ett sådant beslut.

17.4.2 Tillräckliga skyddsåtgärder

Regeringens förslag: Om det inte finns något beslut om adekvat skyddsnivå, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade, eller om den mottagare som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för uppgifterna.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast *Säkerhetspolisen* yttrar sig i denna del och efterfrågar ett förtydligande om uppställande av tredjepartsregeln kan anses som en sådan tillräcklig skyddsåtgärd som föreslås.

Skälen för regeringens förslag: Som utredningen föreslår bör det i den nya lagen tas in en bestämmelse om att personuppgifter får överföras till ett tredjeland eller en internationell organisation, trots att det inte finns ett beslut om adekvat skyddsnivå, om lämpliga skyddsåtgärder säkerställs för personuppgiftsbehandlingen där. Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation ska också vara uppfyllda för att personuppgifter ska få överföras. En motsvarande bestämmelse finns i 8 kap. 4 § brottsdatalagen.

För det första bör lämpliga skyddsåtgärder kunna föreligga om ett avtal säkerställer skyddet för personuppgifter. Ett sådant avtal är dataskyddskonventionen (avsnitt 4.1). Även andra avtal om internationellt samarbete som innehåller bestämmelser om dataskydd och som respekterar registrerades rättigheter kan garantera tillräckligt skydd för personuppgifter som överförs.

För det andra bör personuppgifter få överföras om Säkerhetspolisen har tagit hänsyn till alla omständigheter kring överföringen och dragit slutsatsen att tillräckliga skyddsåtgärder för personuppgifterna föreligger. Vid den bedömningen bör Säkerhetspolisen t.ex. kunna beakta att den som ska behandla personuppgifterna i tredjelandet eller den internationella organisationen kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförs. Även bindande åtaganden om att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt bör kunna beaktas. Det innebär, som *Säkerpolisen* påpekar, att uppställande av tredjepartsregeln bör kunna ge ett tillräckligt skydd för personuppgifterna. Som tidigare har framhållits bygger informationsutbyte mellan underrättelse- och säkerhetstjänster i stor utsträckning på förtroende. Om en underrättelse- eller säkerhetstjänst missbrukar förtroendet blir konsekvensen att den inte längre kommer att få del av relevant information i samma utsträckning

som andra. Det har en självreglerande effekt genom att den mottagande underrättelse- och säkerhetstjänsten måste garantera tillräckligt skydd för uppgifterna för att kunna få del av dem.

17.4.3 Överföringen ska vara nödvändig i en särskild situation

Regeringens förslag: Om det inte finns något beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder får en överföring eller en samling av överföringar av personuppgifter göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig i vissa särskilda undantagssituationer.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs i det enskilda fallet för ett myndighetsintresse eller för att kunna fastslå, göra gällande eller försvara ett rättsligt anspråk.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast *Datainspektionen* yttrar sig och konstaterar att förslaget i denna del innebär en utvidgning i förhållande till nuvarande reglering avseende möjligheten att överföra personuppgifter till tredjeland i särskilda undantagssituationer och efterfrågar analys av eventuella negativa effekter för den personliga integriteteten.

Skälen för regeringens förslag

Överföring är tillåten bara för att tillgodose viktiga intressen

I enskilda fall kan det, trots bristen på skydd för personuppgifter, vara angeläget att kunna föra över vissa personuppgifter till ett tredjeland eller en internationell organisation. Så kan t.ex. vara fallet om Säkerhetspolisen har information om att en misstänkt terrorist befinner sig här i landet men personen identifieras först när han eller hon har rest till ett tredjeland och kan antas komma att begå allvarliga brott där. Säkerhetspolisen har även i vissa fall behov av att kunna utbyta information med underrättelse- och säkerhetstjänster i tredjeländer som har svårt att garantera tillräckligt skydd för personuppgifterna. Det kan gälla vissa särskilda ärenden, situationer eller tidsperioder.

Enligt 8 kap. 5 § brottsdatalagen får en överföring eller en samling av överföringar av personuppgifter göras till ett tredjeland eller en internationell organisation, trots att det inte finns ett beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder, om överföringen är nödvändig i vissa särskilda undantagssituationer. En motsvarande bestämmelse bör tas in i den nya lagen. Samma undantagssituationer bör gälla för Säkerhetspolisen. Dessa behandlas i det följande. Med en samling av överföringar aves bl.a. flera överföringar i ett ärende eller överföringar av samma personuppgifter till flera mottagare samtidigt. Som exempel kan nämnas en utskrift från hemlig avlyssning av elektronisk kommunikation som skickas till ett tredjeland eller en internationell organisation och som

innehålla uppgifter om olika personer som förekommer i en förundersökning (jfr prop. 2017/18:232 s. 381).

Som *Datainspektionen* konstaterar innebär förslaget i denna del en utvidgning av möjligheterna att överföra personuppgifter till tredjeland i särskilda undantagssituationer. Säkerhetspolisen bör inte ha sämre möjligheter än övriga brottsbekämpande myndigheter att överföra uppgifter till tredjeland i undantagssituationer och regleringen bör därför i princip var densamma som enligt brottsdatalagen. Det bör också understrykas att samtliga förutsättningar för överföring alltid ska vara uppfyllda för att personuppgifter ska få överföras. Det gäller alltså även i de särskilda undantagssituationerna.

Enskildas vitala intressen

Enligt 8 kap. 5 § första stycket 1 brottsdatalagen får personuppgifter överföras om det är nödvändigt för att värna den registrerades eller någon annan fysisk persons vitala intressen. I 34 § första stycket d personuppgiftslagen finns en liknande bestämmelse som är tillämplig för Säkerhetspolisen genom en hänvisning i 2 kap. 2 § första stycket 8 och 6 kap. 4 § 1 polisdatalagen. Ett motsvarande undantag bör införas i den nya lagen.

Med vitala intressen bör förstås att det ska vara fråga om ett väsentligt intresse för den enskilde. Det kan röra liv, hälsa eller något annat som är av avgörande betydelse för den enskilde (jfr prop. 2017/18:232 s. 382 f.).

Registrerades berättigade intressen

Personuppgifter får enligt 8 kap. 5 § första stycket 1 brottsdatalagen överföras om det är nödvändigt för att värna den registrerades berättigade intressen. Ett motsvarande undantag bör tas in i den nya lagen. Ordet berättigad förklaras i Svenska Akademiens Ordbok som någon som fått något tilldelat sig eller förvärvat något, eller som är i sin fulla rätt att göra något. Berättigad kan också innebära att något är rättmätigt, välgrundat eller grundat på fullgiltiga skäl. Det behöver alltså inte var fråga om något som är livsviktigt eller annars av avgörande betydelse för den registrerade (prop. 2017/18:232 s. 383).

Myndighetens intresse i enskilda fall

För att inte försvåra brottsbekämpning och lagföring finns i 8 kap. 5 § 2 brottsdatalagen en bestämmelse om att behöriga myndigheter har möjlighet att i enskilda fall överföra personuppgifter till tredjeland eller internationella organisationer trots att landet eller organisationen inte omfattas av ett beslut om adekvat skyddsnivå och det inte heller finns tillräckliga skyddsåtgärder för personuppgifterna. Ett motsvarande undantag bör tas in i den nya lagen, men bör anpassas till Säkerhetspolisens verksamhet. Överföringen bör således vara nödvändig för att i ett enskilt fall kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Rättsliga anspråk i enskilda fall

I 8 kap. 5 § första stycket 3 brottsdatalagen framgår att personuppgifter får överföras om det i ett enskilt fall är nödvändigt för att kunna fastställa,

göra gällande eller försvara ett sådant rättsligt anspråk som hänför sig till ett sådant syfte som omfattas av brottsdatalagens tillämpningsområde. En liknande bestämmelse finns också i 34 § första stycket c personuppgiftslagen, som genom en hänvisning i 2 kap. 2 § första stycket 8 och 6 kap. 4 § 1 polisdatalagen gäller för Säkerhetspolisen. Ett motsvarande undantag bör tas in i den nya lagen.

Allvarlig fara för allmän säkerhet

Det bör tas in en bestämmelse om att personuppgifter får överföras till ett tredjeland eller en internationell organisation, om överföringen är nödvändig för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. En motsvarande bestämmelse finns i 8 kap. 5 § första stycket 4 brottsdatalagen.

Bestämmelsen skulle t.ex. kunna tillämpas om överföringen är nödvändig för att avvärja ett terroristattentat eller en flygplanskapning. Eftersom det typiskt sett är fråga om en överhängande fara för att något ska hända får prövningen i dessa fall göras med utgångspunkt i att åtgärden kan antas vara nödvändig för att avvärja faran. Att faran inte förverkligas behöver inte innebära att överföringen har varit otillåten. Bedömningen måste självfallet göras med hänsyn till vad som är känt när prövningen görs.

En intresseavvägning ska göras i vissa fall

Av 8 kap. 5 § andra stycket framgår att personuppgifter inte får överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs i det enskilda fallet för ett myndighetsintresse eller för att kunna fastslå, göra gällande eller försvara ett rättsligt anspråk. Det bör i den nya lagen, på samma sätt som i brottsdatalagen, ställas krav på en sådan intresseavvägning.

17.5 Överföring till andra mottagare

Regeringens förslag: Säkerhetspolisen ska i ett enskilt fall få överföra personuppgifter till andra mottagare i ett tredjeland än brottsbekämpande myndigheter och underrättelse- och säkerhetstjänster. En sådan överföring ska få göras endast om det är absolut nödvändigt för att Säkerhetspolisen ska kunna utföra vissa arbetsuppgifter och det skulle vara ineffektivt eller olämpligt att överföra personuppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet.

Sådana överföringar ska inte få göras om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Det finns behov av att kunna överföra personuppgifter till andra mottagare

Regleringen i personuppgiftslagen gör ingen skillnad mellan myndigheter och andra mottagare när det gäller överföringar till tredjeland. Säkerhetspolisen kan således enligt den nuvarande regleringen överföra personuppgifter både till myndigheter, andra aktörer och enskilda i tredjeländer om villkoren i övrigt är uppfyllda.

Enligt brottsdatalagen är huvudregeln att överföring ska göras till behöriga myndigheter i det tredje landet. Av förarbetena till brottsdatalagen framgår att myndigheterna har behov av att även kunna överföra personuppgifter till andra än behöriga myndigheter. Där konstateras bl.a. att det finns tillfällen då det underlättar om en svensk myndighet kan överföra personuppgifter till ett tredjeland utan att behöva kanalisera dem via en behörig myndighet i landet. Så kan vara fallet när det rör sig om en särskilt brådskande åtgärd och en kontakt med den behöriga myndigheten riskerar att försena åtgärden eller göra den meningslös (prop. 2017/18:232 s. 292 f). Enligt 8 kap. 8 § brottsdatalagen får överföringar därför göras till andra än behöriga myndigheter om vissa villkor är uppfyllda. Säkerhetspolisen har samma behov som övriga brottsbekämpande myndigheter att i vissa fall kunna överföra personuppgifter till andra mottagare än brottsbekämpande myndigheter eller underrättelse- eller säkerhetstjänster i ett tredjeland. Regeringen delar därför utredningens uppfattning att en liknande bestämmelse bör tas in i den nya lagen. Det innebär att möjligheterna att överföra personuppgifter till andra än brottsbekämpande myndigheter och underrättelse- och säkerhetstjänster begränsas något i förhållande till vad som gäller i dag. Det har dock inte framförts några invändningar mot det. Säkerhetspolisen bör alltså i ett enskilt fall få överföra personuppgifter till en mottagare som inte är en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland om vissa villkor är uppfyllda. Dessa villkor behandlas närmare i det följande.

Överföringen ska vara absolut nödvändig

För att personuppgifter ska få överföras till andra än behöriga myndigheter i ett tredjeland krävs, enligt 8 kap. 8 § första stycket 1 brottsdatalagen, att överföringen ska vara absolut nödvändig för att den svenska myndigheten ska kunna utföra en arbetsuppgift som den har ansvar för och som ligger inom brottsdatalagen tillämpningsområde. Motsvarande bör gälla även för Säkerhetspolisen. Säkerhetspolisen får således endast överföra personuppgifter om det är absolut nödvändigt för att myndigheten ska kunna utföra vissa arbetsuppgifter inom den nya lagens tillämpningsområde. Att överföringen ska vara absolut nödvändig betyder att undantaget ska tillämpas restriktivt och endast i undantagsfall.

Överföring till behörig myndighet är ineffektiv eller olämplig

För att få föra över personuppgifter till någon som inte är en behörig myndighet i ett tredjeland krävs också, enligt 8 kap. 8 § första stycket 3 brottsdatalagen, att det skulle vara ineffektivt eller olämpligt att överföra

uppgifterna till en behörig myndighet där. Enligt förarbetena till brottsdatalagen ligger i det kravet att handläggningen riskerar att fördröjas om uppgifterna överförs till en behörig myndighet. Exempel på när det kan vara ineffektivt att gå via en behörig myndighet i ett tredjeland kan vara överföringar till företag som Google eller Facebook, där det kan röra sig om stora mängder personuppgifter som behöver överföras på kort tid och det kan vara av avgörande betydelse med ett snabbt svar. I undantagsfall kan det också vara olämpligt att överföra en personuppgift via den behöriga myndigheten. Om tidigare kontakter i ärendet med den behöriga myndigheten fått negativa konsekvenser för den svenska myndighetens handläggning bör det kunna vara ett sådant fall. Ett annat exempel är kontakter med ett krigshärjat tredjeland där det kanske inte finns någon behörig myndighet att kommunicera med eller där det är oklart vem som är behörig företrädare för staten. Då är det nödvändigt att kunna överföra personuppgifter till andra än behöriga myndigheter. Det är den överförande myndigheten som ska bedöma om det skulle vara ineffektivt eller på annat sätt olämpligt att överföra personuppgifterna till en behörig myndighet (prop. 2017/18:232 s. 394).

Även enligt den nya lagen bör det vara ett villkor för att få överföra personuppgifter till andra mottagarare i ett tredjeland att det skulle vara ineffektivt eller olämpligt att överföra uppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det landet.

Ingen skyldighet att informera om för vilka ändamål uppgifterna får behandlas

Enligt 8 kap. 8 § andra stycket 2 brottsdatalagen ska den svenska myndigheten informera den som tar emot personuppgifter om de specifika ändamål för vilka uppgifterna får behandlas. Skyldigheten har sin grund i direktivet och har ingen motsvarighet i dag. Frågan är om den även bör gälla för Säkerhetspolisen.

Det finns situationer där det inte är lämpligt att Säkerhetspolisen avslöjar att det är myndigheten som överför viss information. Så kan exempelvis vara fallet när Säkerhetspolisen gör sökningar i vissa utländska databaser som innehåller uppgifter om t.ex. fastigheter eller bolag eller använder liknande tjänster. Sådana sökningar innebär en överföring av personuppgifter till den aktör som ansvarar för databasen eller tjänsten. Säkerhetspolisen kan då i vissa fall behöva dölja att det är myndigheten som gör sökningen. Syftet med informationsskyldigheten är att kunna begränsa den fortsatta användningen av personuppgifterna. Det kan emellertid göras på andra sätt, som inte riskerar att äventyra verksamheten. Något krav på att Säkerhetspolisen alltid ska informera den som tar emot uppgifterna om för vilka ändamål uppgifterna får behandlas eller informera behörig myndighet på det sätt som anges i brottsdatalagen bör därför inte införas.

En intresseavvägning ska göras

Enligt 8 kap. 8 § andra stycket brottsdatalagen får personuppgifter inte överföras till någon som inte är en behörig myndighet i ett tredjeland om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs. På

samma sätt som i brottsdatalagen bör det i den nya lagen föreskrivas att en intresseavvägning ska göras vid överföringar av aktuellt slag. De intressen som ska vägas mot varandra är å ena sidan den registrerades intresse av skydd mot att hans eller hennes rättigheter och friheter kränks genom överföringen och å andra sidan det allmännas intresse av att personuppgifterna överförs. Väger den registrerades intresse av skydd tyngre får överföringen inte göras.

17.6 Villkor för användningen av personuppgifter

Regeringens bedömning: Det behövs inga bestämmelser om användningsbergränsningar i den nya lagen.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att det ska tas in bestämmelser om användningsbegränsningar i den nya lagen.

Remissinstanserna: Det är endast *Säkerhetspolisen* som yttrar sig i denna del. Myndigheten ifrågasätter behovet av att reglera användningsbegränsningar i den nya lagen mot bakgrund av regleringen i lagen (2017:496) om internationellt polisärt samarbete.

Skälen för regeringens bedömning: När en utländsk myndighet överför personuppgifter till en svensk myndighet är det inte ovanligt att den ställer upp användningsbegränsningar. Det kan handla om för vilka ändamål personuppgifterna får användas eller hur länge de får behandlas. Även när en svensk myndighet överför personuppgifter till ett tredjeland eller en internationell organisation finns det ibland skäl att ställa villkor som begränsar användningen av uppgifterna. Att personuppgifterna förses med användningsbegränsningar kan ibland vara en förutsättning för att det ska anses vara lämpligt att överföra uppgifterna (jfr prop. 2017/18:232 s. 397).

Det finns flera författningar som innehåller bestämmelser om sådana användningsbegränsningar, bl.a. 5 kap. 1 § lagen (2000:562) om internationell rättslig hjälp i brottmål, 5 § lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar och 6 kap. 3 och 4 §§ lagen (2017:496) om internationellt polisiärt samarbete. Även i 8 kap. 9 och 10 §§ brottsdatalagen finns bestämmelser om användningsbegränsningar. Att det infördes sådana bestämmelser i brottsdatalagen berodde på att brottsdatalagen har ett vidare tillämpningsområde än de nyss nämnda lagarna, vilket gjorde att bestämmelserna i dem inte var tillräckliga. Utredningen föreslår att motsvarande bestämmelser som i brottsdatalagen ska tas in i den nya lagen. För Säkerhetspolisens del räcker dock bestämmelserna om användningsbegränsningar i de nyss nämnda lagarna. Det finns därför inte skäl att ta in några sådana bestämmelser i den nya lagen.

17.7 Dokumentationskrav och informationsskyldighet

Regeringens bedömning: Skyldigheten att i vissa fall dokumentera överföringar som görs till tredjeland eller internationella organisationer kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* anser att det ska framgå vilka uppgifter som ska dokumenteras vid överföring till tredjeland och internationella organisationer.

Skälen för regeringens bedömning: Enligt 7 kap. 3 § brottsdataförordningen (2018:1202) är behöriga myndigheter i vissa fall skyldiga att dokumentera överföringar till tredjeland och internationella organisationer. Regeringen delar utredningens bedömning att även Säkerhetspolisen bör dokumentera överföringar som gjorts till tredjeland eller internationella organisationer. Det kan regleras i förordning. *Säkerhets- och integritetsskyddsnämndens* synpunkter på förordningsregleringen kommer regeringen att ta ställning till vid utformningen av dessa bestämmelser.

Regeringen delar vidare utredningens bedömning att skyldigheten att självmant informera tillsynsmyndigheten om de överföringar som görs till tredjeland och internationella organisationer riskerar att medföra resurskrävande administrativt arbete för både Säkerhetspolisen och tillsynsmyndigheten. Något sådant krav bör därför inte ställas. I avsnitt 15.5 föreslår regeringen att Säkerhetspolisen ska ge tillsynsmyndigheten tillgång till dokumentation av behandlingen om myndigheten begär det. Det är tillräckligt att dokumentationen görs tillgänglig för tillsynsmyndigheten inom ramen för den skyldigheten.

18 Övriga författningsändringar

Regeringens förslag: Övergångsbestämmelsen i polisens brottsdatalag om att polisdatalagen fortfarande ska gälla för Säkerhetspolisens behandling av personuppgifter i frågor som rör nationell säkerhet, ska upphöra att gälla. Även övergångsbestämmelsen i offentlighets- och sekretesslagen om att äldre föreskrifter fortfarande gäller för sådan verksamhet som avses i 6 kap. 1 § 1 polisdatalagen, ska upphöra att gälla.

I offentlighets- och sekretesslagen, säkerhetsskyddslagen och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning ska hänvisningar till Säkerhetspolisens datalag göras.

Det ska föreskrivas att lagen om internationellt polisiärt samarbete gäller utöver Säkerhetspolisens datalag.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inte att övergångsbestämmelsen i polisens brottsdatalag om att den upphävda polisdatalagen (2010:361) fortfarande

ska gälla för Säkerhetspolisen i vissa delar, ska upphävas. Inte heller att övergångsbestämmelsen i offentlighets- och sekretesslagen (2009:400) om att äldre föreskrifter fortfarande gäller för sådan verksamhet som avses i 6 kap. 1 § 1 polisdatalagen, ska upphävas. Utredningen föreslår inte ändringar i dataskyddslagen eller säkerhetsskyddslagen (2018:585).

Remissinstanserna: *Tidningsutgivarna* tillstyrker förslaget. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

När polisens brottsdatalag infördes upphävdes polisdatalagen. Eftersom Säkerhetspolisens personuppgiftsbehandling på området för nationell säkerhet inte regleras i polisens brottsdatalag behövde polisdatalagen övergångsvis fortsätta att gälla för Säkerhetspolisen i avvaktan på en ny datalag för Säkerhetspolisen. En övergångsbestämmelse av den innebörden infördes därför i polisens brottsdatalag (Brottsdatalagen – kompletterande lagstiftning, prop. 2017/18:269, s. 285). När Säkerhetspolisens nya lag träder i kraft behövs inte längre den övergångsbestämmelsen i polisens brottsdatalag. Den ska därför upphävas.

Vid införandet av polisens brottsdatalag krävdes vidare att vissa bestämmelser i offentlighets- och sekretesslagen, säkerhetsskyddslagen och lagen (2017:496) om internationellt polisiärt samarbete övergångsvis skulle fortsätta att gälla för att Säkerhetspolisen skulle ha möjlighet att behandla personuppgifter på samma sätt som tidigare. Övergångsbestämmelserna i dessa lagar om att äldre föreskrifter fortfarande gäller för uppgifter som behandlas av Säkerhetspolisen med stöd av polisdatalagen, kommer inte längre att gälla när övergångsbestämmelsen i polisens brottsdatalag upphävs. Övergångsbestämmelsen i offentlighets- och sekretesslagen om att äldre föreskrifter fortfarande gäller för sådan verksamhet som avses i 6 kap. 1 § 1 polisdatalagen, måste dock upphävas i samband med att Säkerhetspolisens nya datalag träder i kraft. I samband med att övergångsregleringen upphävs behöver vissa hänvisningar och tillägg göras i de aktuella lagarna.

I 18 kap. 2 § och 35 kap. 1 och 10 §§ offentlighets- och sekretesslagen bör, som utredningen föreslår, hänvisningar göras till Säkerhetspolisens nya datalag. Detta innebär ingen ändring i sak utan är följdändringar i anledning av att Säkerhetspolisen får en ny lag.

I 3 kap. 13 § säkerhetsskyddslagen anges vad som avses med registerkontroll och i 3 kap. 14 § framgår när registerkontroll ska göras. I aktuella paragrafer bör hänvisningar göras till Säkerhetspolisens datalag för att samma reglering som i dag ska gälla. Vidare bör bestämmelsen i 1 kap. 3 § 3 dataskyddslagen som hänvisar till 6 kap. polisdatalagen ändras så att den i stället hänvisar till Säkerhetspolisens nya datalag.

I lagen om internationellt polisiärt samarbete finns bestämmelser om informationsutbyte i 6–10 kap. För att samma reglering ska gälla som i dag för Säkerhetspolisen bör det föreskrivas att lagen ska gälla utöver Säkerhetspolisens datalag. Det innebär att lagen ska tillämpas i den utsträckning den innehåller bestämmelser om personuppgiftsbehandling som avviker från bestämmelserna i Säkerhetspolisens nya lag.

19 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Säkerhetspolisens nya datalag och övriga författningsförslag ska träda i kraft den 1 januari 2020.

Äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som har meddelats före den nya lagens ikraftträdande.

Bestämmelsen om loggning behöver inte tillämpas förrän den 1 oktober 2024 på automatiserade behandlingssystem som har inrättats före den nya lagens ikraftträdande.

I lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska en övergångsbestämmelse införas om att äldre föreskrifter fortfarande gäller för nämndens tillsyn över personuppgiftsbehandling som utförts före ikraftträdandet.

Utredningens förslag överensstämmer delvis med regeringens. När det gäller ärenden om tillsyn enligt personuppgiftslagen som inte avgjorts när den nya lagen träder i kraft föreslår utredningen att äldre bestämmelser om handläggningen ska fortsätta att gälla. Utredningen föreslår även att äldre bestämmelser ska fortsätta att gälla för ärenden om skadestånd för felaktig personuppgiftsbehandling om skadan har orsakats före den nya lagens ikraftträdande. Enligt utredningens förslag behöver bestämmelsen om loggning inte tillämpas förrän den 1 maj 2023 på automatiserade behandlingssystem som har inrättats före den nya lagens ikraftträdande.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag

Ikraftträdande

Säkerhetspolisens nya lag och övriga författningsförslag bör träda i kraft så snart som möjligt. Mot den bakgrunden och med hänsyn till den tid som de olika leden i lagstiftningsprocessen förväntas ta, föreslår regeringen den 1 januari 2020 som tidpunkten för ikraftträdande av den nya lagen och övriga författningsförslag.

Övergångsbestämmelser om tillsyn, skadestånd och överklagande

Det som kan behöva regleras i övergångsbestämmelser till Säkerhetspolisens nya lag – förutom bestämmelser om loggning – är framför allt hur pågående ärenden hos myndigheten och hos tillsynsmyndigheten bör hanteras.

I frågor som rör behandling av personuppgifter hos Säkerhetspolisen bör den nya lagstiftningen tillämpas från det att den träder i kraft. Det innebär exempelvis att framställningar om att få del av information, ärenden om rättelse och andra oavslutade ärenden ska hanteras enligt den nya lagen. Några övergångsbestämmelser för Säkerhetspolisens handläggning behövs därmed inte.

När det gäller tillsynsåtgärder följer det av allmänna principer att förelägganden och förbud som har meddelats med stöd av personuppgiftslagen och som rör den nya lagens tillämpningsområde fortsätter att gälla

efter det att övergångsregleringen i denna del har upphävts. Det behövs därför inte någon särskild övergångsbestämmelse för det.

När det gäller andra frågor om tillsyn över behandling av personuppgifter inom den nya lagens tillämpningsområde föreslår utredningen att äldre bestämmelser ska fortsätta att gälla för de ärenden som har påbörjats före ikraftträdandet, men inte hunnit avgöras när den nya lagen träder i kraft. I propositionen om en ny dataskyddslag (prop. 2017/18:105 s. 175 f.) föreslog regeringen inte någon motsvarande övergångsbestämmelse. Regeringen gjorde bedömningen att det saknas skäl för en sådan övergångsbestämmelse eftersom Datainspektionen påpekat att pågående behandling ska bedömas enligt regleringen i dataskyddsförordningen när den börjar tillämpas (se a. prop. s. 175 f.). Motsvarande bedömning gjordes även i förarbetena till brottsdatalagen (Brottsdatalag, prop. 2017/18:232, s. 424). Mot denna bakgrund anser regeringen att det inte heller nu bör införas någon sådan övergångsbestämmelse till Säkerhetspolisens datalag.

Utredningen föreslår även en övergångsbestämmelse som anger att äldre föreskrifter om skadestånd fortfarande ska gälla för skada som har orsakats före den nya lagens ikraftträdande på grund av felaktig personuppgiftsbehandling inom den nya lagens tillämpningsområde. Det följer emellertid redan av allmänna rättsgrundsatser att ny lagstiftning ska gälla i fråga om skadestånd med anledning av skadefall som inträffar efter ikraftträdandet, medan äldre lag ska tillämpas på skadefall som har inträffat dessförinnan (Kungl. Maj:ts proposition med förslag till skadeståndslag m.m., prop. 1972:5, s. 593 och prop. 2017/18:105 s. 176). Någon särskild övergångsbestämmelse om detta behövs därför inte.

Utredningen föreslår vidare en övergångsbestämmelse om att äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som har meddelats före den nya lagens ikraftträdande och som rör behandling av personuppgifter om nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Regeringen instämmer i utredningens bedömning att en sådan övergångsbestämmelse behövs. Det innebär bl.a. att domstolen vid sin prövning ska tillämpa den äldre lagstiftningen i sådana situationer.

Särskilda övergångsbestämmelser för existerande behandlingssystem

Utredningen föreslår en övergångsbestämmelse enligt vilken den nya bestämmelsen om loggning inte behöver tillämpas förrän den 1 maj 2023 i automatiserade behandlingssystem som Säkerhetspolisen har inrättat före den nya lagens ikraftträdande. En motsvarande övergångsbestämmelse har införts för övriga brottsbekämpande myndigheter i brottsdatalagen (prop. 2017/18:232 s. 427 f.). Bakgrunden är att dataskyddsdirektivet anger att medlemsstaterna får föreskriva detta. Säkerhetspolisen bör få lika lång tid för anpassning av sina it-system som övriga brottsbekämpande myndigheter har fått. Regeringen föreslår därför att det införs en övergångsbestämmelse i Säkerhetspolisens nya lag som innebär att den nya bestämmelsen om loggning inte behöver tillämpas före den 1 oktober 2024. Möjligheten att skjuta upp anpassningen gäller dock bara i fråga om system som har inrättats före ikraftträdandet av lagen.

Övriga lagändringar

Övriga författningsförslag ska gälla från och med att de träder i kraft. I lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet behöver en övergångsbestämmelse införas om att äldre föreskrifter fortfarande gäller för nämndens tillsyn över personuppgiftsbehandling som utförts före ikraftträdandet. Några övriga övergångsbestämmelser behövs inte.

20 Konsekvenser

Regeringens bedömning: Den nya lagen för Säkerhetspolisens personuppgiftsbehandling innebär inga nya arbetsuppgifter för myndigheten, men kommer kräva utbildning av myndighetens personal. Kostnaderna för detta ryms inom Säkerhetspolisens befintliga anslag. Några andra kostnadsökningar för Säkerhetspolisen bedöms förslaget inte medföra.

Polismyndigheten, de allmänna förvaltningsdomstolarna och tillsynsmyndigheterna bedöms endast marginellt påverkas av förslaget. De kostnadsökningar som förslaget kan medföra för dessa kan hanteras inom myndigheternas befintliga anslag. Landsting och kommuner påverkas inte av förslaget.

Förslaget innebär att enskildas rättigheter tydliggörs. Det medför inga ökade kostnader för enskilda.

Informationsutbyte mellan Säkerhetspolisen och andra brottsbekämpande myndigheter kan genom förslaget i vissa fall bli effektivare, vilket är positivt för det brottsförebyggande arbetet.

Förslaget förväntas inte få några andra konsekvenser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Förvaltningsrätten i Stockholm* efterlyser konsekvenserna av att beslut om rättelse, komplettering, radering eller begränsning ska kunna överklagas till allmän förvaltningsdomstol och att tillsynsmyndighetens beslut ska kunna överklagas till förvaltningsdomstol. *Sveriges advokatsamfund* bedömer att det inte är rimligt att utgå ifrån att kostnaderna för genomförandet av förslaget kommer att rymmas inom befintliga anslag och ifrågasätter slutsatsen om att förslaget inte torde medföra några ekonomiska konsekvenser för enskilda. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning

Ett nytt regelverk

Förslaget till ny lag för Säkerhetspolisens personuppgiftsbehandling innebär att Säkerhetspolisen får en modern och skräddarsydd lagstiftning. Regleringen blir betydligt mer omfattande än i dag, men det beror på att den ska vara heltäckande. I stor utsträckning ersätter den nya lagen tidigare lagstiftning. Den nya lagen följer i princip brottsdatalagens systematik och innehåll och innebär att bl.a. bestämmelser om grundläggande krav på

behandling, enskildas rättigheter, skadestånd och rättsmedel i stort överensstämmer med brottsdatalagens bestämmelser.

En alternativ lösning till det som nu föreslås är att reglera Säkerhetspolisens personuppgiftbehandling som rör nationell säkerhet i polisens brottsdatalag. Detta bedöms, som framgår av avsnitt 7.1, som ett sämre alternativ eftersom Polismyndighetens personuppgiftsbehandling i flera delar regleras i brottsdatalagen och merparten av Säkerhetspolisens personuppgiftsbehandling ligger utanför brottsdatalagens tillämpningsområde. Säkerhetspolisen verksamhet förutsätter vidare en delvis annan reglering än Polismyndighetens.

Vilka berörs av förslaget?

Säkerhetspolisen påverkas i första hand av att få en ny lag. Även Polismyndigheten berörs av förslaget liksom förvaltningsdomstolarna, Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Enskilda berörs också av förslaget.

Konsekvenser för Säkerhetspolisen

Även om den nya regleringen av Säkerhetspolisens personuppgiftsbehandling blir mer omfattande än den nuvarande innebär inte förslaget att Säkerhetspolisen tillförs några nya arbetsuppgifter. Vissa av förslagen, framför allt möjligheten att i ökad utsträckning tillhandahålla personuppgifter elektroniskt både genom direktåtkomst och på annat sätt, innebär att Säkerhetspolisens verksamhet kan effektiviseras och lättare möta de ökade kraven på informationsutbyte för att bl.a. bekämpa terrorism. En annan effektivisering är att vissa personuppgifter får behandlas under längre tid än i dag eftersom myndigheten inte i samma utsträckning behöver avsätta resurser för att fatta beslut om förlängning av den tid under vilka uppgifterna får behandlas.

En ny lagstiftning för Säkerhetspolisen kräver utbildningsinsatser inom myndigheten. Det är inte unikt för detta lagstiftningsärende utan uppkommer regelmässig när lagstiftning ändras. Kostnader för utbildning täcks normalt av myndigheternas anslag. Regeringen gör därför bedömningen att kostnaderna för utbildning bör rymmas inom befintliga anslag för Säkerhetspolisen. Ny lagstiftning kräver normalt också nya interna föreskrifter och styrande dokument. Det får anses ingå i de normala uppgifterna för myndigheten.

Förslaget innebär inga skyldigheter för Säkerhetspolisen att inrätta nya it-system. Några kostnader för detta uppkommer således inte med anledning av förslaget. Förslaget bedöms inte heller medföra några ökade kostnader i övrigt för Säkerhetspolisen. Vad *Sveriges advokatsamfund* anfört i denna del ändrar inte denna bedömning.

Konsekvenser för andra myndigheter

Polismyndigheten kommer bara att tillämpa den nya lagen i de fall myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Detta kommer dock ske i ett mycket begränsat antal fall och bedöms inte påverka Polismyndighetens verksamhet i någon större omfattning. De kostnadsökningar som förslaget i denna del kan medföra

för myndigheten bedöms marginella och kan hanteras inom myndighetens befintliga ram.

När det gäller tillsynen över Säkerhetspolisen är förslaget att den i huvudsak bör bedrivas på samma sätt som i dag av Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Förslaget bör därmed inte leda till några merkostnader i denna del för tillsynsmyndigheterna.

Förslaget berör även de allmänna förvaltningsdomstolarna. Möjligheten att överklaga de beslut som nu föreslås finns till viss del redan i dag. Förslaget bedöms inte innebära någon stor måltillströmning och kommer således inte att påverka domstolarnas verksamhet i någon större omfattning. Eventuella kostnadsökningar bedöms kunna hanteras inom befintliga anslag.

Sammantaget bedöms förändringarna för berörda myndigheter inte bli större än att de kan finansieras inom ramen för befintliga anslag. Vad *Sveriges advokatsamfund* anför i denna del föranleder ingen annan bedömning. Motsvarande bedömning gjordes vid införandet av polisens brottsdatalag och övriga registerförfattningar för myndigheterna i rättskedjan (Brottsdatalagen – kompletterande lagstiftning, prop. 2017/18:269, s. 288).

Förslaget bedöms inte påverka några andra statliga myndigheter eller kommuner och landsting.

Konsekvenser för enskilda

Förslaget medför att enskildas rättigheter tydliggörs bl.a. genom att samma krav i princip ställs på Säkerhetspolisen som på andra brottsbekämpande myndigheter.

Förslaget förväntas inte leda till några kostnadsökningar för enskilda. Visserligen föreslås att Säkerhetspolisen i vissa fall ska kunna ta ut avgift för information som begärs, men det är i situationer när den enskilde alltför ofta återkommer med begäran om information. Säkerhetspolisen kan då ge den enskilde informationen mot avgift i stället för att avslå begäran.

Sveriges advokatsamfund anser att de nya regelverken ska uppfattas som att ökade krav ska ställas på skydd för den personliga integriteten och att dessa krav inte kommer att kunna uppfyllas utan sådana åtgärder som medför ekonomiska konsekvenser för enskilda. Regeringen har bedömt att förslagen som gäller brottsdatalagens och övriga registerförfattningars införande inte kan förväntas leda till några sådana kostnadsökningar för enskilda (Brottsdatalagen, prop. 2017/18:232, s. 421 och prop. 2017/18:269 s. 288 f.). Det finns inte heller anledning att förvänta en sådan effekt av det nu aktuella förslaget.

Konsekvenser för det brottsförebyggande arbetet och för brottsligheten

Förslaget kan inte förväntas få några direkta effekter på brottsligheten eftersom det handlar om i huvudsak en administrativ reform. Det innebär dock att Säkerhetspolisen i vissa fall kan utbyta information på ett effektivare sätt, vilket kan få positiva effekter på det brottsförebyggande arbetet.

Förslaget förväntas inte få några konsekvenser i övrigt

Förslaget förväntas inte få några konsekvenser för jämställdheten, det kommunala självstyret eller miljön.

21 Författningskommentar

21.1 Förslaget till lag om Säkerhetspolisens behandling av personuppgifter

1 kap. Allmänna bestämmelser

Syftet med lagen

1 §

Paragrafen reglerar det övergripande syftet med lagen. Övervägandena finns i avsnitt 7.2.

Lagens syfte är dubbelt. Det ena syftet är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter. Det andra syftet är att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt vid brottsbekämpning och lagföring. Det gäller både nationellt och internationellt informationsutbyte.

Lagens tillämpningsområde

2 §

I paragrafen anges lagens tillämpningsområde. Övervägandena finns i avsnitt 7.3 och 7.4.

I *första stycket* anges att lagen gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Vad som är en personuppgift och behandling av personuppgifter definieras i 6 §.

Lagen gäller endast vid behandling av personuppgifter som rör nationell säkerhet. Nationell säkerhet behöver inte avse enbart Sveriges säkerhet. En fråga som rör nationell säkerhet i något av våra grannländer kan t.ex. vara av den karaktären att den även indirekt berör Sveriges nationella säkerhet, exempelvis vid gränsöverskridande terrorism.

I Säkerhetspolisens brottsbekämpande och lagförande verksamhet ingår att förebygga, förhindra och upptäcka brottslig verksamhet och att utreda och beivra, dvs. lagföra, vissa typer av brott. Behandling av personuppgifter i intern och administrativ verksamhet ligger utanför lagens tillämpningsområde.

Av *andra stycket* framgår att lagen gäller vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Det innebär att det som sägs i lagen om Säkerhetspolisen då i stället gäller Polismyndigheten. Bestämmelsen blir tillämplig när Säkerhetspolisen har lämnat över en arbetsuppgift som rör nationell säkerhet till

Polismyndigheten enligt 15 § förordningen (2014:1103) med instruktion för Säkerhetspolisen eller när Säkerhetspolisen begärt bistånd av Polismyndigheten med stöd av 28 § förordningen (2014:1102) med instruktion för Polismyndigheten.

3 §

Paragrafen begränsar lagens tillämpningsområde huvudsakligen till helt eller delvis automatiserad behandling av personuppgifter, men även viss manuell behandling omfattas. Övervägandena finns i avsnitt 7.3.

För att lagen ska vara tillämplig krävs att behandlingen är helt eller delvis automatiserad eller att personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. När det gäller automatiserad behandling krävs det inte att de hanterade personuppgifterna finns i något som kan karaktäriseras som ett register eller att de annars är ordnade på visst sätt. Även behandling av enstaka personuppgifter, t.ex. namn, i löpande text omfattas således av lagens tillämpningsområde. Helt manuell behandling av personuppgifter som inte ingår i någon samling och inte heller är avsedda att ingå i en sådan, exempelvis handskrivna minnesanteckningar, ligger däremot utanför tillämpningsområdet.

Avvikande bestämmelser i annan författning

4 §

Paragrafen reglerar lagens förhållande till avvikande bestämmelser i en annan lag eller en förordning. Övervägandena finns i avsnitt 7.6.

Lagen är subsidiär till annan lagstiftning. Det innebär att om det finns avvikande bestämmelser i t.ex. rättegångsbalken eller lagen (2017:496) om internationellt polisiärt samarbete, gäller de i stället för bestämmelserna i lagen.

Personuppgiftsansvar

5 §

Paragrafen reglerar vem som är personuppgiftsansvarig och personuppgiftsansvarets omfattning. Personuppgiftsansvarig definieras i 1 kap. 6 §. Övervägandena finns i avsnitt 13.1.1 och 13.1.2.

I *första stycket* föreskrivs att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Det gäller även den personuppgiftsbehandling som utförs av personuppgiftsbiträden som myndigheten anlitar. Eftersom Polismyndigheten i vissa fall ska tillämpa lagen föreskrivs det att myndigheten är personuppgiftsansvarig för den behandling som myndigheten utför när den tillämpar lagen.

I *andra stycket* regleras personuppgiftsansvarets omfattning. Bestämmelsen slår fast det helhetsansvar som den personuppgiftsansvarige har och tydliggör hur långt ansvaret sträcker sig när det gäller behandlingen av personuppgifter. Den närmare innebörden av personuppgiftsansvaret framgår av lagens övriga bestämmelser och föreskrifter som meddelas i anslutning till den.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under den personuppgiftsansvariges ledning. Med det avses all personuppgiftsbehandling vid myndigheten. Det gäller både behandling som utförs genom en aktiv handling, t.ex. insamling eller sökning, och passiv behandling, t.ex. lagring. Ansvaret omfattar däremot inte sådan behandling som myndigheten eventuellt utför som personuppgiftsbiträde. Genom att ansvaret knyts till behandling som utförs under den personuppgiftsansvariges ledning tydliggörs att det inte är den personuppgiftsansvarige, dvs. myndigheten, som utför personuppgiftsbehandlingen utan de anställda.

Den personuppgiftsansvarige är också ansvarig för all behandling av personuppgifter som utförs på dennes vägnar. Med det avses främst sådan behandling som den personuppgiftsansvarige har uppdragit åt ett personuppgiftsbiträde att utföra. Den personuppgiftsansvarige kan uppdra åt ett biträde att utföra viss behandling av personuppgifter, men kan inte genom det avsäga sig personuppgiftsansvaret. Personuppgiftsansvaret sträcker sig då utanför den personuppgiftsansvariges egen verksamhet. Personuppgiftsbiträdens behandling ska styras av skriftliga avtal eller andra skriftliga överenskommelser och får endast utföras enligt instruktioner från den personuppgiftsansvarige, se kommentarerna till 5 kap. 11 och 13 §§.

Två eller flera personuppgiftsansvariga kan behandla samma personuppgifter samtidigt för olika ändamål, t.ex. om de har direktåtkomst till personuppgifter i samma system. Varje personuppgiftsansvarig är då ansvarig för den behandling som utförs under dennes ledning eller på dennes vägnar.

Definitioner

6 §

I paragrafen definieras olika uttryck som används i lagen.

Behandling av personuppgifter

Uttrycket behandling av personuppgifter omfattar alla åtgärder som vidtas med sådana uppgifter. Så snart personuppgifter hanteras på något sätt är det fråga om behandling som omfattas av lagens bestämmelser, om den är helt eller delvis automatiserad eller avser manuell behandling i en strukturerad samling av personuppgifter. Uppräkningen i definitionen av olika sätt att hantera personuppgifter är således inte uttömmande. Uttrycket behandlas i avsnitt 7.7.

Biometriska uppgifter

Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på fysiska karaktärsdrag hos den som ska identifieras. Mönster av fingeravtryck, ansiktsgeometri, ögats iris, regnbågshinna och näthinna, röst, hand, blodkärl, dna eller gång är exempel på områden där sådan teknik kan användas. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Uppgifterna kan användas för att skapa en

referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. Fingeravtryck är en vanlig form av biometrisk uppgift. Personuppgifter, t.ex. fingeravtryck, som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska uppgifter utgör däremot inte biometriska uppgifter.

Biometriska uppgifter i form av fingeravtryck kan framgå av ett spår som påträffas vid utredning av ett brott. Även analys av spåren omfattas av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Dna-spår behandlas i kommentaren till uttrycket genetiska uppgifter.

Av 2 kap. 10 § framgår att biometriska uppgifter som används i syfte att identifiera en person är känsliga personuppgifter som bara får behandlas om det är absolut nödvändigt.

Fotografier och filmer som inte bearbetas tekniskt i syfte att åstadkomma unik identifiering faller utanför definitionen. Bearbetning av bilder av personer för att förbättra bildkvaliteten, förstärka detaljer och liknande omfattas alltså inte. Om bilder däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram i syfte att identifiera personer omfattas de av definitionen. Att fotografier kan omfattas av regleringen av känsliga personuppgifter på andra grunder behandlas i kommentaren till 2 kap. 9 §. Uttrycket behandlas i avsnitt 7.7.

Dataskyddsombud

Ett dataskyddsombud är en fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att person-uppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen. Ett dataskyddsombud ska enligt lagen vara anställd hos Säkerhetspolisen, se 5 kap. 9 §. Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden förutsätts framför allt ha goda kunskaper om reglerna om personuppgiftsbehandling. Ombuden bör också ha sådan ställning i organisationen att deras synpunkter och råd tas på allvar. Dataskyddsombudens uppgifter regleras i 5 kap. 10 §. Uttrycket behandlas i avsnitt 13.3.1.

Genetiska uppgifter

All information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från t.ex. en brottsplats eller ett prov från människokroppen omfattas av definitionen.

Genetiska uppgifter behandlas vid dna-analyser i forensisk verksamhet för att ta fram dna-profiler eller forensiska uppslag. Behandlingen kan avse genetiska uppgifter från såväl identifierade som oidentifierade personer. Eftersom nedärvda eller förvärvade genetiska kännetecken för en person kan framgå av ett spår som påträffas vid utredning av ett brott, omfattas även analys av spåren av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Själva dna-profilen utgör däremot inte en genetisk uppgift eftersom inga nedärvda eller förvärvade genetiska kännetecken kan utläsas ur den. Uttrycket behandlas i avsnitt 7.7.

I 28 kap. 12–12 b §§ rättegångsbalken finns bestämmelser om provtagning för dna-analys. Av 2 kap. 10 § denna lag framgår att Säkerhetspolisen inte får behandla genetiska uppgifter.

Internationell organisation

Med internationell organisation avses dels organisationer och deras underställda organ som lyder under folkrätten, dels andra organ som inrättats genom eller på grundval av överenskommelser mellan två eller flera stater. Interpol och Världstullorganisationen (World Customs Organization) är exempel på internationella organisationer som omfattas av definitionen. Internationella domstolar och tribunaler som t.ex. Internationella brottmålsdomstolen, Internationella krigsförbrytartribunalen för det forna Jugoslavien och Tribunalen för Libanon ska också betraktas som internationella organisationer. Uttrycket behandlas i avsnitt 17.2.

Mottagare

Mottagare definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Undantaget omfattar bl.a. myndigheter som tar del av personuppgifter i sin tillsyn över viss verksamhet, t.ex. Datainspektionen och Säkerhets- och integritetsskyddsnämnden som båda utövar tillsyn över personuppgiftsbehandling. Även andra myndigheter som utövar tillsyn, t.ex. Justitieombudsmannen och Justitiekanslern, omfattas av undantaget. Uttrycket behandlas i avsnitt 7.7.

Personuppgift

Med personuppgift avses varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Uttrycket behandlas i avsnitt 7.7.

Varje upplysning som kan hänföras till en fysisk person är en personuppgift. Det gäller även upplysningar som kan hänföras till en individ om en fysisk person kan identifieras med hjälp av informationen. Det krävs inte att den personuppgiftsansvarige ska förfoga över samtliga uppgifter som gör identifieringen möjlig. Det innebär att t.ex. oidentifierade fingeravtryck och dna-profiler är personuppgifter, eftersom det är möjligt att identifiera en person med hjälp av dem. Även bild- eller ljudupptagningar kan utgöra personuppgifter, om man direkt eller indirekt kan avgöra vilken individ som upptagningen avser.

Definitionen omfattar bara uppgifter om personer som är i livet. Det innebär att behandling av uppgifter om avlidna eller ännu inte födda personer inte omfattas av lagen. Av lagen (1987:269) om kriterier för bestämmande av människans död och lagen (2005:130) om dödförklaring framgår när någon ska betraktas som avliden. Däremot omfattar definitionen uppgifter om vem som är släkt med den avlidne.

Uppgifter om juridiska personer omfattas inte av definitionen.

Personuppgiftsansvarig

Personuppgiftsansvarig är enligt definitionen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Uttrycket behandlas i avsnitt 13.1.1.

Att bestämma ändamålen med behandlingen innebär i princip att bestämma att en behandling ska utföras och varför. Att bestämma medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen, dvs. hur behandlingen ska gå till. Det kan handla om vilka personuppgifter som ska behandlas, vilka som ska få ta del av dem och hur länge personuppgifterna får behandlas. Den personuppgiftsansvarige styr dock inte alltid själv över alla medel för behandlingen. Vid direktåtkomst bestämmer den som medger åtkomsten hur tillgången tekniskt ska lösas och vilka personuppgifter som ska tillgängliggöras. Den som ges direktåtkomst är personuppgiftsansvarig för behandlingen av de personuppgifter som direktåtkomsten avser.

Det framgår av 1 kap. 5 § att Säkerhetspolisen och Polismyndigheten är personuppgiftsansvarig enligt lagen.

Personuppgiftsbiträde

Ett personuppgiftsbiträde är en fysisk eller juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning. Uttrycket behandlas i avsnitt 13.4.1

Ett personuppgiftsbiträde behandlar personuppgifter endast enligt instruktioner från den personuppgiftsansvarige och har inte rätt att själv bestämma över personuppgiftsbehandlingen. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen, t.ex. kan en myndighet behandla personuppgifter som personuppgiftsbiträde åt en annan myndighet. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

Registrerad

Med registrerad avses den fysiska person som en personuppgift rör. Av definitionen av personuppgift framgår bl.a. att personen ska vara i livet. Uttrycket behandlas i avsnitt 7.7.

Tredjeland

Tredjeland definieras som en stat som inte är medlem i Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning. Förutom medlemsstaterna i EU är det Island, Liechtenstein, Norge och Schweiz som inte är tredjeland i lagens mening.
Uttrycket behandlas i avsnitt 17.2.

Tredje man

Tredje man definieras som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och

sådana personer som under den personuppgiftsansvarige eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Uttrycket behandlas i avsnitt 14.3.2.

Uppgift som rör hälsa

Med uppgift som rör hälsa avses en personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus. Av 2 kap. 9 § framgår att uppgifter som rör hälsa är känsliga personuppgifter som bara får behandlas under vissa förutsättningar. Uttrycket behandlas i avsnitt 7.7.

Behandling av uppgifter om juridiska personer

7 §

I paragrafen anges vilka bestämmelser i lagen som gäller för behandling av uppgifter om juridiska personer. Övervägandena finns i avsnitt 7.8.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Rättsliga grunder

1 §

Paragrafen reglerar tillsammans med 2 § de tillåtna rättsliga grunderna för Säkerhetspolisens behandling av personuppgifter. Övervägandena finns i avsnitt 8.3.1.

I paragrafen anges den yttre ramen för när behandling av personuppgifter är tillåten. Paragrafen motsvarar i huvudsak 6 kap. 1 § polisdatalagen (2010:361), men är numera inte en ändamålsbestämmelse enligt de skäl som anges i avsnitt 8.2.

Av *första stycket* framgår att personuppgifter får behandlas om det är nödvändigt för att Säkerhetspolisen ska kunna utföra vissa uppgifter, vilka räknas upp i punkterna 1–5. Nödvändighetsrekvisitet innebär att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt. Behandling av personuppgifter definieras i 1 kap. 6 §.

Enligt *punkt 1 a–c* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet, terrorbrott eller tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv. Brott mot Sveriges säkerhet brukar anses innefatta bl.a. sådana brott som avses i 18 och 19 kap. brottsbalken. Med terrorbrott avses brott mot lagen (2003:148) om straff för terroristbrott, lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall och lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Med uttrycket förebygga, förhindra eller upptäcka brottslig verksamhet avses framför allt Säkerhetspolisens underrättelseverksamhet. I sådan verksamhet samlas information in, analyseras och bearbetas i syfte att

förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts (prop. 2009/10:85 s. 318). Om det finns misstankar om ett konkret brott kan personuppgifter behandlas för att utreda brottet enligt punkt 2.

I punkt 1 ingår bl.a. myndighetens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag. Insamling av uppgifter om verksamheter och annat som kan utvecklas till konkreta hot mot det svenska samhället eller mot enskilda personer i statsledningen är ett annat exempel. Även spaning i syfte att uppdaga sådan brottslig verksamhet som Säkerhetspolisen bekämpar hör hit (prop. 2009/10:85 s. 362 f.).

Under punkt 1 ryms också handläggning av frågor om tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet är att förhindra brott. Personuppgiftsbehandling vid annan brottsförebyggande verksamhet omfattas också.

Enligt *punkt 2* får personuppgifter behandlas i syfte att utreda eller lagföra sådana brott som avses i punkt 1. Vidare omfattas utredning och lagföring av brott i de fall där Säkerhetspolisen har hand om eller är delaktig i en brottsutredning efter särskilt beslut.

Att utreda brott innebär framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses konkreta brott, men det kan vara fråga om såväl brott som bevisligen har begåtts som brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Även personuppgiftsbehandling vid åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken omfattas. Under denna punkt ligger också det biträde som Säkerhetspolisen ger åklagare i förundersökningar, vilket även inkluderar hanteringen av hemliga tvångsmedel. Även spaning under förundersökning hör hit, liksom användning av överskottsinformation för att utreda brott (prop. 2009/10:85 s. 363).

Enligt *punkt 3 a* får Säkerhetspolisen behandla personuppgifter för att fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer. Det innefattar exempelvis behandling av uppgifter rörande den skyddade personen själv, personer i hans eller hennes närmaste krets och andra personer som han eller hon kommer i kontakt med och uppgifter om personer som kan utgöra hot mot den skyddade personen. Det är inte enbart uppgifter som behövs för att skyddsuppgiften ska kunna fullgöras som får behandlas med stöd av denna punkt. Den omfattar även behandlingen av personuppgifter för själva bevaknings- och säkerhetsarbetet, exempelvis uppgifter om vem som fullgör bevakningsuppgiften vid ett visst tillfälle (prop. 2009/10:85 s. 363).

Punkt 3 b ger Säkerhetspolisen möjlighet att behandla personuppgifter för att fullgöra uppgifter som anges i säkerhetsskyddslagen (2018:585). I uppgifterna ingår bl.a. registerkontroll och utlämnande av uppgifter med anledning av sådan kontroll.

I *punkt 3 c* regleras Säkerhetspolisens personuppgiftsbehandling för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen. Det som avses är framför allt Säkerhetspolisens personuppgiftsbehandling i s.k. säkerhetsärenden enligt utlänningslagen (2005:716), men även i verkställighetsärenden enligt den lagen. Säkerhetspolisen har också uppgifter enligt lagen (1991:572) om särskild utlänningskontroll och lagen (2001:82) om svenskt medborgarskap. Personuppgiftsbehandling i sådana ärenden omfattas också.

I *punkt* 4 föreskrivs att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för att utföra en annan uppgift som rör nationell säkerhet, om uppgiften anges i lag eller förordning eller särskilt beslut av regeringen.

Punkt 5 reglerar den personuppgiftsbehandling som krävs för att Säkerhetspolisen ska kunna fullgöra förpliktelser som följer av internationella åtaganden. Till dem hör bl.a. att skydda vissa företrädare för utländska stater som besöker Sverige, främst statsöverhuvuden och regeringsföreträdare. I den mån personuppgiftsbehandling vid skyddet av dem inte regleras i punkt 3 a, t.ex. därför att skyddet i huvudsak fullgörs av utländsk säkerhetspersonal, regleras det i denna punkt.

Behandlingen enligt denna punkt tar också sikte på sådana förpliktelser som syftar till att gagna utländsk brottsbekämpande verksamhet. Säkerhetspolisen lämnar, i likhet med Polismyndigheten, i viss utsträckning andra länder hjälp i brottsutredningar. Punkten omfattar den behandling av personuppgifter som behövs för det. Den täcker också Säkerhetspolisens informations- och erfarenhetsutbyte med motsvarande myndigheter i andra stater, i den mån utbytet grundar sig på ett internationellt åtagande. Om informationsutbytet äger rum enbart i svenskt intresse hör det normalt hemma under någon av de andra punkterna. Däremot hör sådant informationsutbyte som enbart gagnar den utländska myndigheten, t.ex. uppgifter om brott i en annan stat, hemma under denna punkt (prop. 2009/10:85 s. 363 f.).

2 §

Paragrafen reglerar, tillsammans med 1 §, de tillåtna rättsliga grunderna för behandling av personuppgifter enligt lagen. I paragrafen regleras två särskilt angivna fall där det är tillåtet att behandla personuppgifter oberoende av om förutsättningarna för behandling enligt 1 § föreligger. Den motsvarar tidigare 6 kap. 3 § polisdatalagen (2010:361). Tillämpningsområdet för paragrafen är begränsat eftersom det enbart är personuppgifter som lämnats till Säkerhetspolisen som får behandlas. Övervägandena finns i avsnitt 8.3.2.

Enligt *punkt 1* får personuppgifter alltid behandlas om behandlingen är nödvändig för diarieföring. Normalt finns det en rättslig grund enligt 1 § för Säkerhetspolisens diarieföring. Den nu aktuella punkten täcker behovet av att kunna diarieföra handlingar i andra fall. Det kan även röra sig om muntliga uppgifter som nedtecknas i en tjänsteanteckning eller liknande. Vilka uppgifter som måste noteras i samband med diarieföring av en handling framgår av 5 kap. 2 § offentlighets- och sekretesslagen (2009:400). Vid diarieföring av inkomna handlingar får det således alltid anges vem en handling har kommit från och i korthet vad handlingen rör.

Någon annan behandling än sådan som är nödvändig för diarieföringen får emellertid inte utföras med stöd av denna punkt. Den fortsatta behandlingen ska således – utom i fall där andra punkten i denna paragraf blir tillämplig – alltid ha stöd i 1 §.

Personuppgifter får enligt *punkt 2* alltid behandlas om de har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning. Uttrycket ”anmälan, ansökan eller liknande” innefattar alla slag av framställningar till Säkerhetspolisen. Det gäller både skriftliga framställningar och uppgifter som lämnas muntligen, men nedtecknas av någon hos myndigheten. Oftast omfattas framställningar av detta slag av bestämmelsen om rättslig grund i 1 § och ska då behandlas med stöd av den bestämmelserna, men i vissa fall kan innehållet i handlingen vara sådant att nödvändighetsrekvisitet i den paragrafen inte är uppfyllt. Eftersom det vanligtvis krävs något slag av handläggning hos Säkerhetspolisen för att hantera en framställan, har det tidigare ansetts behövas en särskild bestämmelse för personuppgiftsbehandling i dessa fall (prop. 2009/10:85 s. 324). Behandlingen måste vara nödvändig för handläggningen. Det kan i ett enskilt fall innebära att personuppgifter i ett e-postmeddelande inte får behandlas på annat sätt än att uppgifterna tas emot och därefter omedelbart arkiveras eller gallras. I ett annat fall kan bestämmelsen innebära att personuppgifterna också får behandlas i samband med att framställningen besvaras.

Ändamål

3 §

I paragrafen regleras kravet på särskilt, uttryckligt angivna och berättigade ändamål för behandling av personuppgifter och behandling för nya ändamål. Övervägandena finns i avsnitt 8.4.1 och 8.4.2.

Av *första meningen* framgår att ändamålen för behandling av personuppgifter ska vara särskilda, uttryckligt angivna och berättigade. Ändamålen måste bestämmas redan när uppgiften behandlas första gången och får inte blandas ihop med den rättsliga grunden för behandling. Ändamålet ska vara mer konkret.

Att ändamålet ska vara särskilt innebär att det måste vara tillräckligt preciserat för att det ska kunna avgöras om de personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen eller om för många personuppgifter behandlas. Ändamålet får alltså inte vara så vagt eller vittomfattande att någon sådan prövning i praktiken inte blir möjlig. Ett pågående underrättelsearbete om viss, närmare angiven brottslig verksamhet kan utgöra ett ändamål. Eftersom Säkerhetspolisens personuppgiftsbehandling till övervägande del utförs i myndighetens underrättelseverksamhet är det inte alltid möjligt att i ett tidigt stadium av processen ange ändamålen för behandlingen lika preciserat som i annan brottsbekämpande verksamhet. Inledningsvis kan därför ändamålen behöva anges mer övergripande för att sedan konkretiseras.

Att ändamålet ska vara berättigat innebär en koppling till de rättsliga grunderna. Personuppgifter får inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden. Personuppgifter som avser en förundersökning får t.ex. inte längre behandlas för det ändamålet när brottet har preskriberats.

I *andra meningen* framgår att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål personuppgifterna ursprungligen behandlades för, vilket ger uttryck för den s.k. finalitetsprincipen. När Säkerhetspolisen ska behandla personuppgifter för nya ändamål måste myndigheten alltid pröva om det nya ändamålet är förenligt med det ändamål som personuppgifterna samlades in för. Eftersom Säkerhetspolisens verksamhet är inriktad på att bekämpa brott som till sin natur är systemhotande kan behandling av personuppgifter för nya ändamål inom den egna organisationen i de allra flesta fall anses förenlig med ursprungsändamålet.

4 §

Paragrafen reglerar för vilka ändamål Säkerhetspolisen får behandla personuppgifter för att tillgodose behovet av information i annan verksamhet. Övervägandena finns i avsnitt 8.4.3.

Behandling enligt denna paragraf förutsätter att personuppgifterna redan är föremål för behandling med stöd av 1 §. Paragrafen motsvarar 6 kap. 2 § polisdatalagen (2010:361).

I *första stycket* ges Säkerhetspolisen stöd för att behandla personuppgifter för att kunna lämna ut dem till bl.a. andra brottsbekämpande myndigheter. Behandling av personuppgifter definieras i 1 kap. 6 §.

Enligt *punkt 1* får Säkerhetspolisen, vars brottsbekämpning rör ett relativt begränsat område, utföra den behandling som krävs för att till rätt myndighet vidarebefordra bl.a. uppgifter om brott eller brottslig verksamhet som Säkerhetspolisen upptäcker, men själv saknar behörighet att handlägga (prop. 2009/10:85 s. 365).

Punkt 2 ger Säkerhetspolisen stöd för att behandla uppgifter för att lämna ut dem till en annan myndighet inom ramen för myndighetsöverskridande samverkan mot brott. I första hand tillgodoser punkten behovet av informationsutbyte med andra myndigheter än brottsbekämpande eftersom punkt 1 i huvudsak täcker det behovet.

Enligt *punkt 3* får Säkerhetspolisen behandla personuppgifter för att kunna lämna ut dem till Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller till Försvarets radioanstalts försvarsunderrättelseverksamhet. Vad försvarsunderrättelseverksamhet är framgår av kommentaren till 3 kap. 6 §. Enligt punkten får Säkerhetspolisen behandla personuppgifter som den anser kan vara värdefulla för någon av dessa myndigheter och vill vidarebefordra dit. Möjligheterna till sådan behandling begränsas genom kravet på att det ska finnas särskilda skäl att tillhandahålla informationen (prop. 2009/10:85 s. 365 f.).

Enligt *punkt 4* får Säkerhetspolisen behandla personuppgifter om myndigheten enligt lag eller förordning har till uppgift att bistå en annan myndighet med en viss uppgift. Punkten omfattar bl.a. den behandling som kan krävas för att Säkerhetspolisen ska kunna bistå Riksdagens ombudsmän eller Justitiekanslern med uppgifter när de uppträder som förundersökningsledare och åklagare (prop. 2014/15:94 s. 137).

Enligt *punkt 5* får information som behandlas med stöd av 1 § också behandlas för att tillhandahålla information som är nödvändig för den brottsbekämpande verksamheten vid en utländsk myndighet eller en

mellanfolklig organisation (prop. 2009/10:85 s. 366). I 16 § finns en sekretessbrytande bestämmelse som möjliggör sådant utlämnande.

Punkt 6 ger Säkerhetspolisen möjlighet att behandla personuppgifter för att lämna ut dem till en utländsk underrättelse- eller säkerhetstjänst om det inte täcks av någon av de övriga punkterna i paragrafen.

Av *andra stycket* framgår att personuppgifter får behandlas om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. Vad bestämmelsen innebär utvecklas i propositionen Integritet och effektivitet i polisens brottsbekämpande verksamhet (prop. 2009/10:85 s. 323 och 366).

I *tredje stycket* tydliggörs att de i paragrafen angivna ändamålen inte är uttömmande. För att en uppgift ska få vidarebehandlas för något annat ändamål än de som anges i första och andra styckena måste det emellertid i det enskilda fallet göras en bedömning att det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

5 §

I paragrafen föreskrivs att Säkerhetspolisen får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Övervägandena finns i avsnitt 8.4.4.

Paragrafen reglerar bara Säkerhetspolisens behandling för statistiska, vetenskapliga eller historiska ändamål inom lagens tillämpningsområde och gäller inte för exempelvis Brottsförebyggande rådets statistikverksamhet. Den gäller heller inte Säkerhetspolisens behandling av personuppgifter för syften utanför lagens tillämpningsområde.

Vid behandling för de i paragrafen angivna ändamålen ska lagens övriga bestämmelser tillämpas på samma sätt som vid annan behandling enligt lagen. De uppgifter som behandlas ska vara adekvata och relevanta och inte för omfattande i förhållande till det vetenskapliga, statistiska eller historiska ändamålet. På samma sätt som man vid behandling för andra ändamål inom lagens tillämpningsområde måste se till att uppgifterna inte behandlas under längre tid än vad som behövs, får uppgifter som behandlas för statistiska, vetenskapliga eller historiska ändamål inte behandlas under längre tid än vad som behövs för dessa ändamål.

Författningsenlig och korrekt behandling

6 §

I paragrafen föreskrivs att personuppgifter alltid ska behandlas författningsenligt och på ett korrekt sätt. Övervägandena finns i avsnitt 9.1.1.

När det är tillåtet att behandla personuppgifter och vilka krav som ställs på behandlingen framgår inte bara av denna lag och föreskrifter som har meddelats med stöd av den, utan också av andra författningar som reglerar t.ex. särskilda register. Regler av nu aktuellt slag har betydelse för bedömningen av både om behandlingen är författningsenlig och vad som är ett korrekt sätt att behandla personuppgifter. I det ligger bl.a. kravet på att det ska göras en kontinuerlig bedömning av att personuppgiftsbehandlingen uppfyller alla formella krav.

Vad som är ett korrekt sätt för behandling styrs emellertid inte bara av författningsregler och den praxis som utbildas kring dem. Tillsynsmyndighetens allmänna råd och uttalanden i fråga om personuppgiftsbehandling har också betydelse, liksom Säkerhetspolisens interna regler.

Otillåten behandling av personuppgifter kan i vissa fall vara straffbar enligt bestämmelser i brottsbalken, bl.a. regeln om dataintrång i 4 kap. 9 c §. Det kan då röra sig om externa angrepp eller om att någon som har tillgång till ett it-system överskrider sina befogenheter.

Personuppgifternas kvalitet

7 §

Paragrafen reglerar hur personuppgifter som behandlas ska vara beskaffade. Övervägandena finns i avsnitt 9.1.2.

I *första stycket* föreskrivs att de personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

En personuppgift är korrekt om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är får man söka ledning i ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses. Inom lagens tillämpningsområde måste frågan om en personuppgift är korrekt inte bara vägas mot ändamålen med behandlingen utan även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. För att kunna avgöra om personuppgifterna är korrekta är det också av stor betydelse att veta om de grundar sig på fakta eller på personliga bedömningar. Kravet på att personuppgifter ska vara korrekta innebär inte något hinder mot att samla in exempelvis osäkra underrättelseuppgifter, under förutsättning att personuppgifterna är relevanta för arbetet (se 8 §) och att det framgår att det är osäkert om uppgiften är riktig.

De personuppgifter som behandlas behöver bara vara uppdaterade om det är nödvändigt. Frågan om det är nödvändigt att de är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen. Exempelvis kan uppgifter om telefonnummer eller andra kontaktuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras. När ärendet har avslutats eller arkiverats är det dock inte nödvändigt att uppdatera kontaktuppgifter.

I *andra stycket* föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet. Syftet med bestämmelsen är att förhindra att personers utseende beskrivs i ordalag som kan vara kränkande för individen. Utformningen av bestämmelsen innebär att Säkerhetspolisen alltid är oförhindrad att, när den får ett tips från allmänheten om en person som kan misstänkas för brott, göra de anteckningar som är nödvändiga för att underlätta identifieringen av personen, t.ex. anteckningar om fysiska kännetecken. I anslutning till dessa anteckningar får även sådana känsliga personuppgifter som avses i 9 § första stycket antecknas, om det är absolut nödvändigt för det arbete som tipset kan komma att leda till.

8 §

Paragrafen reglerar omfattningen av behandlingen av personuppgifter. Övervägandena finns i avsnitt 9.1.2.

Av paragrafen framgår att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och att fler personuppgifter inte får behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses.

Att personuppgifterna ska vara adekvata och relevanta innebär att ovidkommande uppgifter inte får behandlas. En prövning av om en personuppgift är nödvändig för behandlingen ska göras kontinuerligt av Säkerhetspolisen, inte bara när uppgiften registreras eller på annat sätt samlas in. Även vid en senare behandling ska personuppgiften behövas för just den behandlingen, annars är kravet på adekvans och relevans inte uppfyllt.

Förutom att uppgifterna ska vara adekvata och relevanta får de inte heller vara fler än nödvändigt. Det understryker kravet på att en fortlöpande bedömning görs.

Det kan vara svårare att bedöma om uppgifterna är adekvata och relevanta i Säkerhetspolisens verksamhet än i annan polisverksamhet, eftersom det som regel inte är lika tydligt vari den brottsliga verksamheten eller säkerhetshotet består. Vid bedömningen av mängden personuppgifter som behöver behandlas i förhållande till ändamålet kan hänsyn också behöva tas till andra aspekter än enbart behoven i det enskilda fallet. För att pågående underrättelse- eller utredningsverksamhet inte ska avslöjas kan Säkerhetspolisen ibland behöva behandla fler uppgifter än vad som krävs i ett visst ärende, för att inte avslöja vem eller vilka som myndigheten intresserar sig för. Kravet på att uppgifterna ska vara adekvata och relevanta och inte för många i förhållande till ändamålet med behandlingen får i dessa fall ändå anses vara uppfyllt.

Känsliga personuppgifter

9 §

Paragrafen reglerar tillsammans med 10–12 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Att uppgifterna betecknas som känsliga personuppgifter framgår av 11 §. Övervägandena finns i avsnitt 9.2.1.

Enligt *första stycket* får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte behandlas. Det innebär att det inte är tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda på den grunden att de utifrån etniskt ursprung, politiska åsikter eller något annat i paragrafen angivet förhållande kan hänföras till en viss kategori av människor.

En uppgift om utseende är normalt inte en känslig personuppgift och den får alltså behandlas, med den begränsning som följer av 7 § andra stycket. Om en sådan uppgift samtidigt innebär uppgift om etniskt ursprung omfattas den dock av förbudet. Bestämmelsen hindrar inte att uppgifter om en persons nationalitet behandlas, eftersom en sådan uppgift normalt inte ger upplysning om etniskt ursprung (prop. 2009/10:85 s. 325). Uppgifter om att en viss person kommer från en viss världsdel eller ett visst land faller också som regel utanför förbudet mot behandling av

känsliga personuppgifter. Skulle en sådan personuppgift i det enskilda fallet t.ex. avslöja etniskt ursprung är dock förbudet tillämpligt.

Avbildningar av personer, inte minst fotografier, kan avslöja många detaljer. Man kan t.ex. se hudfärg eller om personen bär klädsel eller andra kännetecken som är typiska för utövare av en viss religion. Även fysiska funktionsnedsättningar kan framgå av bilder och det kan även framgå att en person är sjuk eller skadad. Bilder på människor i mera normala sammanhang torde inte avslöja känsliga personuppgifter, medan bilder på människor som utövar religiösa, politiska eller sexuella aktiviteter som regel utgör känsliga personuppgifter (jfr Öman m.fl. s. 288).

I *andra stycket* görs det undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Uppgifter om en person som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för ändamålet med behandlingen. Det innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får de kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung om det är av betydelse för utredningen. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste dock behovet av att göra sådana kompletteringar prövas noga i det enskilda fallet.

Känsliga personuppgifter kan också förekomma i Säkerhetspolisens verksamhet på grund av att någon under ett förhör har lämnat en sådan uppgift eller i en inlaga nämnt uppgiften. Det kan vara fråga om helt grundlösa påståenden eller påståenden som inte har någon relevans i sammanhanget. Eftersom myndigheterna inte kan hindra någon från att yttra sig vare sig muntligen eller skriftligen kan känsliga personuppgifter på detta sätt komma att ingå i t.ex. en förundersökning. Om det nedtecknade förhöret eller den inkomna handlingen ingår i förundersökningen omfattas behandlingen av den känsliga personuppgiften även i dessa fall av undantaget i detta stycke.

10 §

I paragrafen regleras när biometriska uppgifter får behandlas. Övervägandena finns i avsnitt 9.2.1.

Biometriska uppgifter, som definieras i 1 kap. 6 §, är känsliga personuppgifter och får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen. Det innebär att behovet av att behandla sådana uppgifter måste prövas särskilt noga.

Paragrafen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Det innebär att t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster får användas för att identifiera en person.

Genetiska uppgifter, som definieras i 1 kap. 6 § och som också är känsliga personuppgifter, får Säkerhetspolisen inte behandla.

11 §

Paragrafen reglerar tillsammans med 9, 10 och 12 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Övervägandena finns i avsnitt 9.2.1.

I paragrafen klargörs att sådana personuppgifter som avses i 9 och 10 §§ utgör känsliga personuppgifter. Vidare tydliggörs att sådana uppgifter alltid får behandlas i de fall som avses i 2 §, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i en anmälan, ansökan eller liknande, om det är nödvändigt för Säkerhetspolisens handläggning. Det innebär bl.a. att det är möjligt för myndigheten att ta emot och besvara anmälningar, ansökningar och liknande skrifter som lämnas i elektronisk form även om de innehåller känsliga personuppgifter. Regleringen innebär också att sådana uppgifter får arkiveras om det är nödvändigt. Som framgår av kommentaren till 2 § är den behandling som är tillåten begränsad.

12 §

Paragrafen reglerar användningen av känsliga personuppgifter vid sökning. Övervägandena finns i avsnitt 9.2.2. Av 9 och 10 §§ framgår vilka personuppgifter som är känsliga personuppgifter.

Enligt *första stycket* är det som huvudregel förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har viss politisk eller religiös åskådning eller sexuell läggning. Uppgifter som beskriver en persons utseende, t.ex. uppgifter om längd, hudfärg eller tatueringar, får användas som sökbegrepp så länge syftet med sökningen inte är att göra en sammanställning av en viss grupp av personer grundad på exempelvis etniskt ursprung eller politisk åskådning.

Även tillåtna sökningar kan resultera i ett urval av personer grundat på känsliga personuppgifter, t.ex. sökningar som görs i registervårdande syfte. I vilken utsträckning det sedan är tillåtet att behandla någon eller några av personuppgifterna i sammanställningen får prövas mot huvudregeln för behandling av känsliga personuppgifter i 9 §.

I *andra stycket* görs det undantag från sökförbudet i första stycket. Undantaget gäller både vid sökning i personuppgifter som har gjorts gemensamt tillgängliga och i personuppgifter som inte har det. Sökförbudet hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, eller uppgifter som beskriver en persons utseende används som sökbegrepp, även om det skulle leda till ett urval av personer grundat på känsliga personuppgifter som t.ex. hälsa eller sexuell läggning.

Med uppgifter som beskriver en persons utseende avses signalementsuppgifter som t.ex. kroppsbyggnad, ansiktsform, hår- och hudfärg, klädsel och fysiska kännetecken som födelsemärken, blindhet och tatueringar (jfr prop. 2011/12:45 s. 124). En sökning på ett fysiskt särdrag kan ge ett urval av personer grundat på uppgifter som rör hälsa.

Sökning på t.ex. vissa tillvägagångssätt vid brott kan resultera i ett urval av personer grundat på sexualliv eller sexuell läggning. Uppgifter om tatueringar kan t.ex. avslöja viss politisk åsikt eller religiös övertygelse.

Enligt *tredje stycket* hindrar sökförbudet inte sökningar i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för de syften som anges i

1 §. Säkerhetspolisen kan behöva söka på uppgifter som rör politiska åsikter, religiös övertygelse eller etniskt ursprung, eftersom det ingår i Säkerhetspolisens uppdrag att kartlägga sådan verksamhet som kan komma att hota vitala samhällsfunktioner och att skydda statsledningen. Sådana sökningar kan även behöva göras t.ex. för att förebygga och förhindra tryck- eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv.

Kravet på att det ska vara absolut nödvändigt att göra sökningen gör att utrymmet för sådana sökningar är begränsat och att rutinmässiga sökningar på känsliga uppgifter inte är tillåtna.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 9 §. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Rättelse, uppdatering och radering

13 §

I paragrafen föreskrivs vad Säkerhetspolisen ska göra för att förhindra att felaktiga eller ofullständiga personuppgifter behandlas, lämnas ut eller görs tillgängliga. Övervägandena finns i avsnitt 9.3.

I paragrafen föreskrivs att alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Vad som avses med att uppgifter är korrekta framgår av kommentaren till 7 §. Säkerhetspolisen ska också utan onödigt dröjsmål uppdatera uppgifter som är inaktuella om det är nödvändigt. Bestämmelsen innebär att Säkerhetspolisen självmant måste vidta åtgärder för att säkerställa personuppgifternas kvalitet. I 6 kap. 6 § regleras vad som gäller när den registrerade själv begär att personuppgifter ska rättas eller kompletteras.

Vad som utgör rimliga åtgärder skiljer sig åt beroende på om personuppgifterna är felaktiga, ofullständiga eller inaktuella eftersom personuppgifter alltid ska vara korrekta, men endast behöver vara uppdaterade om det är nödvändigt. Vilka åtgärder som är rimliga att vidta får bedömas mot bakgrund av omständigheterna i varje enskilt fall, som t.ex. ändamålet med behandlingen, vilka personuppgifter som behandlas och vilka konsekvenser en felaktig eller ofullständig uppgift kan få för den enskilde.

14 §

I paragrafen föreskrivs vilka åtgärder som ska vidtas om personuppgifter behandlas på ett otillåtet sätt. Övervägandena finns i avsnitt 9.3.

I *första stycket* föreskrivs att alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–10 § utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller när radering krävs för att Säkerhetspolisen ska utföra en rättslig förpliktelse. När radering kan komma i fråga, förutsättningarna för

det och vad som kan vara en rättslig förpliktelse utvecklas i kommentaren till 6 kap. 7 §.

I stället för att personuppgifter som behandlas på ett otillåtet sätt raderas ska enligt *andra stycket* behandlingen av uppgifterna utan onödigt dröjsmål begränsas om uppgifterna behöver finnas kvar av bevisskäl. Vad det innebär utvecklas i kommentaren till 6 kap. 7 §.

I 6 kap. 7 § regleras vad som gäller när den registrerade begär att motsvarande åtgärder ska vidtas.

Utlämnande av personuppgifter

15 §

Paragrafen reglerar utlämnande av personuppgifter som är nödvändiga för att framställa rättsstatistik. Sådana uppgifter ska enligt paragrafen lämnas till den som ansvarar för att framställa sådan statistik. Enligt 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet ansvarar myndigheten för kriminalstatistiken. Övervägandena finns i avsnitt 11.4.4

16 §

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organisationer (prop. 2009/10:85 s. 329 f.). Övervägandena finns i avsnitt 11.4.3.

Sekretessen bryts och personuppgifter får enligt *första stycket* lämnas ut till någon av de mottagare som anges i *punkt 1* om mottagaren behöver dem för att kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott. Enligt *punkt 2* får personuppgifter lämnas till en utländsk underrättelse- eller säkerhetstjänst. Personuppgifterna får bara lämnas ut enligt första och andra punkten om det är förenligt med svenska intressen.

Enligt *andra stycket* kan Säkerhetspolisen lämna ut uppgifter till en utländsk myndighet eller mellanfolklig organisation om utlämnandet följer av en internationell överenskommelse som Sverige tillträtt.

Vid överföring av personuppgifter till tredjeland ska regleringen i 9 kap. också tillämpas.

17 §

Genom paragrafen bryts viss sekretess som annars skulle ha gällt gentemot Polismyndigheten. Övervägandena finns i avsnitt 11.4.2.

Polismyndigheten har enligt paragrafen rätt att, trots viss angiven sekretess till skydd för enskild, få del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar med stöd av 2 kap. 1 § första stycket 1–3 a och c om Polismyndigheten behöver uppgifterna för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Motsvarande gäller om Polismyndigheten behöver uppgifterna för att fullgöra sina uppgifter enligt utlänningslagen (2005:716) eller lagen (1991:572) om särskild utlänningskontroll. Det är Säkerhetspolisen som avgör om Polismyndigheten behöver uppgifterna.

18 §

Genom paragrafen bryts viss sekretess som annars skulle ha gällt gentemot Försvarsmakten och Försvarets radioanstalt. Övervägandena finns i avsnitt 11.4.2.

I paragrafen regleras Försvarsmaktens och Försvarets radioanstalts rätt att, trots viss angiven sekretess till skydd för enskild, få del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar med stöd av 2 kap. 1 § första stycket 1 eller 2. En förutsättning för att uppgifter ska få lämnas ut är att uppgifterna behövs i försvarsunderrättelseverksamheten eller den militära säkerhetstjänsten hos Försvarsmakten eller i försvarsunderrättelseverksamheten hos Försvarets radioanstalt. I kommentaren till 3 kap. 6 § utvecklas vad försvarsunderrättelseverksamhet är. Det är Säkerhetspolisen som avgör om Försvarsmakten och Försvarets radioanstalt behöver uppgifterna.

19 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt. Övervägandena finns i avsnitt 11.2 och 11.3.1.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med elektroniskt utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring, på ett usb-minne eller annat motsvarande medium.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (prop. 2014/15:148 s. 113).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter. Är det fråga om processmaterial som översänds till parter eller ombud bör även principen om parternas likställdhet i processen beaktas.

Frågan om elektroniskt utlämnande till enskilda är särskilt svårbedömd när det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Om det kan antas att personuppgifterna efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen eller dataskyddslagen om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter ska lämnas ut elektroniskt bör även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får Säkerhetspolisen inte efterforska syftet med

begäran, vilket kan ha betydelse vid prövningen av om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt.

Andra stycket innehåller en upplysning om att direktåtkomst endast är tillåten i den utsträckning som anges i lagen.

Personuppgifter från transportföretag

20 §

Paragrafen reglerar tillsammans med 21 § hur personuppgifter som ett transportföretag tillhandahåller enligt 25 § polislagen (1984:387) får behandlas. Övervägandena finns i avsnitt 9.4.

Regleringen avser uppgifter om ankommande eller avgående transporter av bl.a. passagerare och fordon som transportföretag befordrar till och från Sverige. Det rör sig alltså om bokningsuppgifter i framför allt flyg- och färjetrafik. Transportföretagens skyldighet att tillhandahålla uppgifterna regleras i polislagen.

I lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen regleras personuppgiftsbehandling som avses i den lagen. Om den lagen eller föreskrifter som regeringen har meddelat i anslutning till lagen innehåller avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag. Detta följer av 1 kap. 4 §.

I *första stycket* tydliggörs att uppgifter från transportföretag får behandlas i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Enligt *andra stycket* får personuppgifter som avses i första stycket bara i enskilda fall behandlas för nya ändamål. Ett typiskt exempel är att uppgifterna behövs i ett visst underrättelseärende.

Det framgår av 3 kap. 2 § i vilken utsträckning som personuppgifter från transportföretag får göras gemensamt tillgängliga.

21 §

I paragrafen anges hur uppgifter från transportföretag som tillhandahålls genom terminalåtkomst får behandlas. Paragrafen motsvarar delvis den tidigare bestämmelsen i 26 § andra stycket polislagen (1984:387). Övervägandena finns i avsnitt 9.4.

Paragrafen reglerar enbart behandling vid terminalåtkomst till personuppgifter hos transportföretag, medan 20 § anger vad som gäller i fråga om personuppgifter som förs över till Säkerhetspolisens it-system eller behandlas strukturerat på annat sätt.

Genom terminalåtkomsten till företagens it-system får Säkerhetspolisen tillgång till omfattande överskottsinformation om resande. Myndigheten får inte ändra eller på annat sätt bearbeta uppgifter i sådana system. Syftet med regleringen är att myndigheten inte heller ska kunna föra över en hel sådan uppgiftssamling till sitt egna it-system för att bearbeta, ändra och lagra personuppgifterna där. Som framgår av 20 § får uppgifter däremot i enskilda fall behandlas för nya ändamål om förutsättningarna för det är uppfyllda.

Rätt att meddela föreskrifter

22 §

I paragrafen finns en upplysning om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 15–18 §§ och om begränsning av möjligheterna att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Övervägandena finns i avsnitt 11.2 och 11.4.2.

3 kap. Gemensamt tillgängliga uppgifter

Allmän bestämmelse

1 §

Av paragrafen framgår att kapitlet innehåller särskilda bestämmelser om gemensamt tillgängliga uppgifter. Vad som avses med att uppgifter görs gemensamt tillgängliga utvecklas i propositionen Integritet och effektivitet i polisens brottsbekämpande verksamhet (prop. 2009/10:85, s. 369). Övervägandena finns i avsnitt 10.1.

I *första stycket* anges att kapitlet bara gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga med stöd av 2 §. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter. I kommentaren till 2 kap. 2 § redogörs närmare för vilken personuppgiftsbehandling som får ske vid diarieföring eller i fråga om uppgifter som lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande handling.

Personuppgifter som får göras gemensamt tillgängliga

2 §

Av paragrafen framgår att personuppgifter får göras gemensamt tillgängliga om det behövs för någon av de arbetsuppgifter som Säkerhetspolisen får behandla personuppgifter för och som anges 2 kap. 1 §. Övervägandena finns i avsnitt 10.1.

Särskilda upplysningar

3 §

I paragrafen föreskrivs att det ska anges för vilket ändamål gemensamt tillgängliga uppgifter behandlas, om detta inte framgår av sammanhanget eller på något annat sätt. Övervägandena finns i avsnitt 10.2.

Om det ändamål för vilket gemensamt tillgängliga personuppgifter behandlas för inte framgår av sammanhanget eller på annat sätt ska det tydliggöras genom en särskild upplysning. Behandlas uppgifterna i en förundersökning eller i ett ärende framgår ändamålet normalt sett av sammanhanget. Det gäller också många gånger om uppgifterna finns i ett

särskilt register eller i en viss uppgiftssamling som skapats för ett visst ändamål.

4 §

I paragrafen regleras i vilken utsträckning gemensamt tillgängliga uppgifter ska förses med särskilda upplysningar. Övervägandena finns i avsnitt 10.2 och 10.3.

Enligt *första stycket* ska gemensamt tillgängliga uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet förses med en särskild upplysning om det, om det inte på annat sätt framgår att personen inte är misstänkt. Det kan t.ex. framgå att personen är uppgiftslämnare. Det ska alltså gå att skilja mellan personer som är föremål för Säkerhetspolisens intresse på grund av inblandning i brottslig verksamhet och personer som inte är misstänkta för det. Genom hänvisningen till 2 kap. 1 § första stycket 1 eller 2 klargörs att upplysningen ska avse brott eller brottslig verksamhet som Säkerhetspolisen har till uppgift att bekämpa.

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med sådan brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Kravet på särskild upplysning gäller bara uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med någon annan som är misstänkt för att utöva sådan brottslig verksamhet eller rör sig i en miljö där brottslighet förekommer utan att ha naturliga skäl att befinna sig där. Uppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller utanför, utom i de fall där båda kan antas ha direkt samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som är misstänkt för att utöva eller komma att utöva brottslig verksamhet som behöver förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt fråga om uppgifter som belyser brottslighetens art och omfattning. Uppgifterna kan då behöva förses med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Det krävs inte någon upplysning om det på grund av omständigheterna är onödigt. Utrymmet för att underlåta att förse uppgifter med upplysning om trovärdighet och riktighet har därmed utökas något i förhållande till dagens reglering genom att det inte längre krävs särskilda omständigheter för att upplysningskravet inte ska gälla. Det är tillräckligt att det på grund av de samlade omständigheterna framstår som obehövligt att förse uppgifterna med en upplysning. Det kan vara fallet om uppgiftslämnaren är en polisman eller någon annan vars trovärdighet är väl känd. Även i sådana fall kan det behövas en särskild upplysning om uppgifternas riktighet i sak.

Av *tredje stycket* framgår att uppgifter som ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har tillgång till, inte behöver förses med någon

upplysning enligt andra stycket om bearbetningen inte har genomförts. Undantaget innebär att personuppgifter i en sådan uppgiftssamling får göras gemensamt tillgängliga trots att de inte har hunnit förses med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Så snart bearbetningen är genomförd och uppgifterna kopplats till annan information måste personuppgifterna kompletteras med sådana upplysningar om det behövs.

Undantaget är kopplat till om bearbetningen av uppgifterna är genomförd. Hur lång tid det kan ta kan variera beroende på bl.a. mängden information och uppgifternas karaktär. Utgångspunkten är att bearbetningen ska genomföras så snart som möjligt.

I 4 kap. 8 § anges hur länge uppgifter i en sådan uppgiftssamling får behandlas.

Direktåtkomst

5 §

I paragrafen föreskrivs att Polismyndigheten under vissa förutsättningar får medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar. Övervägandena finns i avsnitt 11.3.2.

Direktåtkomsten får bara avse personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar de brott som anges i 2 kap. 1 § 1, utreda eller lagföra brott sådana brott eller fullgöra uppgifter i samband med personskydd eller enligt utlännings- och medborgarskapslagstiftningen.

Möjligheten att ge Polismyndigheten direktåtkomst begränsas till personuppgifter som behövs för något av de syften som anges i 2 kap. 1 § första stycket 1 och 2 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller för att fullgöra uppgifter enligt utlänningslagen (2005:716) eller lagen (1991:572) om särskild utlänningskontroll. Det innebär att Polismyndigheten bara får ta del av uppgifter genom direktåtkomst för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott samt för att fullgöra uppgifter enligt de två övriga lagarna som nämns. Det sistnämnda kan exempelvis avse informationsutbyte i samband med att Polismyndigheten verkställer beslut om avvisning eller utvisning i säkerhetsärenden enligt utlänningslagen. Om Polismyndigheten behöver få tillgång till personuppgifter för att utföra andra arbetsuppgifter ska uppgifterna lämnas på något annat sätt.

Paragrafen innebär inte att Polismyndigheten har rätt till direktåtkomst. En bestämmelse om direktåtkomst anger endast i vilken form personuppgifter får tillhandahållas. Det är Säkerhetspolisen som avgör om personuppgifterna kan tillhandahållas genom direktåtkomst. Säkerhetspolisen kan begränsa direktåtkomsten till t.ex. en viss typ av uppgifter eller på annat sätt som myndigheten finner lämpligt. Möjligheten att tillhandahålla vissa personuppgifter på detta sätt kan också vara begränsad av att uppgifterna är skyddade av sekretess. Se vidare 2 kap. 17 § gällande sekretessgenombrott i vissa fall.

6 §

I paragrafen anges att Försvarets radioanstalt och Försvarsmakten under vissa förutsättningar får medges direktåtkomst till personuppgifter som behandlas av Säkerhetspolisen. Övervägandena finns i avsnitt 11.3.2.

Försvarets radioanstalt får medges direktåtkomst inom ramen för försvarsunderrättelseverksamheten, medan Försvarsmakten utöver försvarsunderrättelseverksamheten också får medges direktåtkomst inom den militära säkerhetstjänsten. Försvarsunderrättelseverksamhet bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten får bara avse utländska förhållanden (jfr 1 § lagen (2000:130) om försvarsunderrättelseverksamhet).

Direktåtkomsten för Försvarsmakten och Försvarets radioanstalt får bara avse personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar de brott som anges i 2 kap. 1 § 1 samt för att utreda eller lagföra brott sådana brott.

Paragrafen innebär inte att de mottagande myndigheterna har rätt till direktåtkomst. En bestämmelse om direktåtkomst anger endast i vilken form personuppgifter får lämnas ut. Säkerhetspolisen avgör om myndigheten kan medge Försvarsmakten och Försvarets radioanstalt direktåtkomst. Direktåtkomsten kan begränsas till t.ex. en viss typ av uppgifter eller på annat sätt som Säkerhetspolisens finner lämpligt. Möjligheten att tillhandahålla vissa uppgifter på detta sätt kan också vara begränsas av att uppgifterna är skyddade av sekretess. Se vidare 2 kap. 18 § gällande sekretessgenombrott i vissa fall.

7 §

I paragrafen regleras Säkerhetspolisens möjlighet att medge underrättelse- och säkerhetstjänster inom Europeiska unionen (EU) och Europeiska ekonomiska samarbetsområdet (EES) direktåtkomst till vissa personuppgifter. Övervägandena finns i avsnitt 11.3.3.

I *första stycket* anges förutsättningarna för när direktåtkomst kan medges. Det är endast tillåtet att medge underrättelse- och säkerhetstjänster i medlemsstater inom EU och EES direktåtkomst och de får endast medges direktåtkomst om det behövs för samarbetet mot terrorism. Direktåtkomsten får vidare bara avse personuppgifter som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott. Direktåtkomsten får endast avse personuppgifter som gjorts gemensamt tillgängliga.

Innan Säkerhetspolisen medger direktåtkomst med stöd av denna bestämmelse måste myndigheten dels avgöra om det finns sakliga skäl att låta en utländsk underrättelse- och säkerhetstjänster få del av uppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att bekämpa terrorism, dels avgöra om det finns rättsliga förutsättningar för att lämna ut uppgifterna. I detta ingår att en sekretessprövning görs. Se vidare 2 kap. 16 § gällande sekretessgenombrott i vissa fall.

Av *andra stycket* framgår att Säkerhetspolisen ska informera regeringen innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt paragrafen. Skyldigheten att informera regeringen

omfattar enbart det förhållandet att Säkerhetspolisen avser att dela information genom direktåtkomst, inte innehållet i informationen.

Rätt att meddela föreskrifter

8 §

I paragrafen finns en upplysning om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om omfattningen av direktåtkomst och om behörighet och säkerhet vid sådan åtkomst. Övervägandena finns i avsnitt 11.3.2.

Kap. 4 Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 §

Paragrafen reglerar hur länge Säkerhetspolisen får behandla personuppgifter för ändamål inom lagens tillämpningsområde. Där framgår också hur bestämmelsen förhåller sig till arkivlagstiftningen. Övervägandena finns i avsnitt 12.2.1.

I *första stycket* föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det som avses är ändamålet i det enskilda fallet. Ibland behandlas personuppgifter för flera olika ändamål. Att det inte längre finns behov av att behandla personuppgiften för ett visst ändamål medför inte att behandlingen av den måste upphöra för alla andra ändamål samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål inte att den får fortsätta att behandlas för alla ändamål lika länge. Behovet av att fortsätta att behandla uppgifterna måste prövas kontinuerligt. Om det är tillräckligt att behandla avidentifierade uppgifter är det inte längre tillåtet att behandla personuppgifterna.

Av *andra stycket* framgår att bestämmelsen om längsta tid för behandling inte hindrar att personuppgifterna arkiveras av Säkerhetspolisen eller att arkivmaterial lämnas till en arkivmyndighet. Behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde.

I *tredje stycket* föreskrivs att övriga bestämmelser i kapitlet, som anger hur länge en viss typ av personuppgifter får behandlas inom den ram som sätts av huvudregeln i första stycket, endast gäller vid automatiserad behandling.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 §

I paragrafen anges hur länge uppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Övervägandena finns i avsnitt 12.2.2.

I *första stycket* anges hur länge uppgifterna får behandlas.

Enligt *andra stycket* gäller inte bestämmelsen i 1 § andra stycket vid tillämpningen av denna paragraf. Det innebär att personuppgifterna inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av uppgifterna ska upphöra när den tid som anges i paragrafen

har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges paragrafen (jfr 12 §).

Tredje stycket klargör att paragrafen inte ska tillämpas på ärenden om utredning av eller lagföring för brott (se 3–5 §§).

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 §

Paragrafen reglerar hur länge personuppgifter i en anmälan om brott får behandlas (jfr prop. 2009/10:85 s. 346 f.). Övervägandena finns i avsnitt 12.2.5.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen. Bestämmelserna hindrar alltså inte att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen.

4 §

Paragrafen reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas (jfr prop. 2009/10:85 s. 347 f.). Övervägandena finns i avsnitt 12.2.5.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen. Bestämmelserna hindrar alltså inte att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen.

5 §

Paragrafen reglerar vad som gäller i fråga om personuppgifter som rör någon som har varit misstänkt i en förundersökning som har lagts ner eller där åtal har lagts ner eller frikännande dom har meddelats och fått laga kraft. Övervägandena finns i avsnitt 12.2.5.

Övriga gemensamt tillgängliga uppgifter

6 §

I paragrafen anges att det i de följande paragraferna regleras hur länge gemensamt tillgängliga uppgifter som inte förekommer i ärenden om utredning av eller lagföring för brott får behandlas. Övervägandena finns i avsnitt 12.2.1.

I *första stycket* finns en upplysning om att de aktuella personuppgifterna som längst får behandlas under den tid som anges i 7–10 §§.

Enligt *andra stycket* gäller inte bestämmelsen i 1 § andra stycket om arkivlagstiftningens företräde vid tillämpningen av 7–10 §§. Det innebär att personuppgifterna inte får arkiveras digitalt. Utgångspunkten är att all automatiserad behandling av uppgifterna ska upphöra när den tid som anges i 7–10 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort.

Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de aktuella paragraferna (jfr 12 §).

7 §

Paragrafen reglerar hur länge sådana personuppgifter som avses i 6 § får behandlas. Övervägandena finns i avsnitt 12.2.3.

Huvudregeln i *första stycket* innebär att personuppgifter som har gjorts gemensamt tillgängliga inte får behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Tiden för hur länge personuppgifterna får behandlas kan inte påverkas av vilken registrering som helst, exempelvis kan en registrering av ändrade bostadsförhållanden eller något annat liknande förhållande inte påverka hur länge uppgifterna får behandlas.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock enligt *andra stycket* inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge. Femårsfristen gäller bara registreringar som har gjorts innan den unge fyllt 18 år. Om nya uppgifter om honom eller henne registreras därefter, förlängs tidsfristen för alla uppgifter enligt huvudregeln i första stycket.

I *tredje stycket* görs undantag från bestämmelserna i första och andra stycket för personuppgifter som avses i 8 och 9 §§, dvs. personuppgifter som behandlas i en uppgiftsamling som har skapats för att bearbeta och analysera information och personuppgifter som rör viss säkerhetshotande verksamhet.

8 §

Paragrafen reglerar hur länge personuppgifter i sådana särskilda uppgiftssamlingar som anges i 3 kap. 4 § tredje stycket får behandlas. Övervägandena finns i avsnitt 12.2.3.

Personuppgifter i en uppgiftssamling som skapats för att bearbeta och analysera information får inte behandlas längre än tre efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen. Om nya uppgifter om personen samlas in förlängs tidsfristen, under förutsättning att uppgifterna är av den art att de påverkar hur länge personuppgifterna får behandlas. Vad det innebär utvecklas i kommentaren till 7 §.

9 §

I paragrafen anges hur länge personuppgifter som hänför sig till viss säkerhetshotande verksamhet får behandlas. Övervägandena finns i avsnitt 12.2.4.

Uppgifter som hänför sig till sådan säkerhetshotande verksamhet som anges i paragrafen kan t.ex. vara uppgifter där grunden för registreringen är att personen antas vara en utländsk underrättelseofficer och uppgifter om hans eller hennes anhöriga. Det kan också vara uppgifter om personer som misstänks för spionerі eller andra brott enligt 18 och 19 kap. brottsbalken som främmande makt står bakom och om personer med anknytning

till dem. Registreringen kan även avse händelser kopplade till dessa personer.

Personuppgifter som omfattas av paragrafen får behandlas längst 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Tidsfristen gäller dock inte uppgifter som behandlas i sådana särskilda uppgiftssamlingar som anges i 3 kap. 4 § tredje stycket. Sådana uppgifter får inte behandlas längre än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen (se 8 §).

10 §

I paragrafen ges Säkerhetspolisen möjlighet att, om det finns särskilda skäl, genom ett beslut i det enskilda fallet förlänga tidsfristen för behandlingen av vissa personuppgifter. Ett särskilt skäl kan vara att ärendet rör en företeelse eller en person som kan antas få ny aktualitet (prop. 2009/10:85 s. 269). Övervägandena finns i avsnitt 12.2.6.

Tidsfristerna om tio respektive tre år motsvarar den tidigare regleringen. Även om personuppgifterna rör någon som inte har fyllt 18 år är tidsfristen tio år. Detsamma gäller för sådana personuppgifter som anges i 9 §.

Rätt att meddela föreskrifter

11 §

I paragrafen finns en upplysning om att regeringen kan meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom lagens tillämpningsområde under längre tid än vad som anges i 3 och 4 §§. En förutsättning för sådana föreskrifter är att de tidsfrister som sätts för behandlingen hålls inom de ramar som ges i 1 § första stycket. Övervägandena finns i avsnitt 12.3.

12 §

I paragrafen finns en upplysning om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om att personuppgifter, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål. Regeringen, eller den myndighet som regeringen bestämmer, kan också meddela föreskrifter om begränsning av behandlingen av personuppgifter för ändamål inom lagens tillämpningsområde vid digital arkivering. Övervägandena finns i avsnitt 12.3.

5 kap. Skyldigheter som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

1 §

Paragrafen reglerar tillsammans med 2–4 §§ de krav som ställs på Säkerhetspolisen i fråga om tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter är

författningsenlig och att registrerades rättigheter skyddas. Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 7 §. Övervägandena finns i avsnitt 13.2.2.

Organisatoriska åtgärder som avses i paragrafen är bl.a. att anta interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av it-system, behandlingar och vidtagna åtgärder samt teknisk spårbarhet genom loggning och logguppföljning.

Vilka åtgärder som bör vidtas får avgöras efter en bedömning i de enskilda fallen. Vid den bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga de är. Även grunden för behandlingen och riskerna med den ska beaktas. Mer långtgående åtgärder kan behövas vid behandling som kan medföra särskilda risker för integritetsintrång eller vid omfattande behandling av en stor mängd personuppgifter.

Skyldigheten att vidta lämpliga åtgärder är inte knuten till en viss tidpunkt, utan något som Säkerhetspolisen ständigt ska ha för ögonen. Åtgärder som har vidtagits måste därför kontinuerligt revideras och vid behov förändras.

2 §

Paragrafen reglerar skyldigheten att beakta principen om inbyggt dataskydd vid behandling av personuppgifter. Övervägandena finns i avsnitt 13.2.2.

Paragrafen innebär att Säkerhetspolisen, både när medlen för behandlingen bestäms och vid behandlingen, ska vidta åtgärder som medför att dataskyddsprinciper säkerställs och skyddsåtgärder integreras i behandlingen. Skyldigheten är nära förknippad med de skyldigheter som följer av 1, 3 och 7 §§. Paragrafen kan ses som en precisering av den övergripande skyldigheten i 1 §.

Exempel på grundläggande dataskyddsprinciper som bör säkerställas är uppgiftsminimering, dvs. att så få personuppgifter som möjligt samlas in och hanteras, och att personuppgifter inte behandlas längre än vad som behövs eller används på ett otillåtet sätt. Principerna kan säkerställas i verksamheten genom åtgärder som exempelvis begränsar behandlingen till personuppgifter som endast indirekt pekar ut en individ eller till personuppgifter som är mindre integritetskänsliga. Att använda pseudonymisering, vilket innebär att uppgifterna inte går att koppla till en enskild person utan ytterligare information som hålls avskild, är ett annat exempel. Om det i ett ärendehanteringssystem är möjligt att behandla personuppgifterna utöver vad som är tillåtet med hänsyn till ändamålet bör funktionerna begränsas och spärras innan systemet tas i drift. Funktioner för att avskilja personuppgifter automatiskt är också exempel på inbyggt dataskydd. Andra åtgärder som kan vidtas för att säkerställa dataskydds-principer är behörighetsstyrning och kryptering av information. Sådana åtgärder syftar till att begränsa åtkomsten till personuppgifterna så att endast de som behöver uppgifterna för att kunna utföra sina arbetsuppgifter har tillgång till dem.

Integrering av skyddsåtgärder kan avse funktioner för autentisering, t.ex. lösenord, möjlighet att använda kryptering vid kommunikation över internet och på mobila enheter, funktioner för loggning och säkerhetskopiering.

Vilka åtgärder som bör vidtas får avgöras i varje enskilt fall. Vilka faktorer som kan vara av betydelse utvecklas i kommentaren till 1 §. De tekniska möjligheterna och kostnaderna för genomförandet ska också vägas in.

3 §

Paragrafen fastställer Säkerhetspolisen skyldighet att i automatiserade behandlingssystem införa dataskydd som standard. Övervägandena finns i avsnitt 13.2.2.

Dataskydd som standard innebär att systemet automatiskt styr användaren mot att arbeta integritetssäkert. Grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas. Skyldigheten att ha dataskydd som standard tar sikte på mängden insamlade personuppgifter, behandlingens omfattning, hur länge personuppgifterna behandlas och hur tillgängliga de är. Det innebär att Säkerhetspolisen ska se till att det i automatiserade behandlingssystem endast är möjligt att samla in de typer av personuppgifter som behövs, att personuppgifterna endast kan behandlas på ett sådant sätt och så länge som det är nödvändigt och att uppgifterna endast är tillgängliga för de personer som behöver dem i sitt arbete. Paragrafen kan i likhet med 2 § ses som en precisering av den övergripande skyldigheten i 1 §.

Med automatiserade behandlingssystem avses särskilt för verksamheten utformade eller anpassade behandlingssystem där personuppgifter behandlas mer eller mindre strukturerat, t.ex. verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. För att dataskydd som standard ska kunna införas i automatiserade behandlingssystem krävs det att Säkerhetspolisen har tekniska möjligheter och rätt att vidta sådana åtgärder i systemet. Standardprogram som Word, Outlook och Excel är inte att anse som automatiserade behandlingssystem i paragrafens mening och omfattas därför inte av kraven.

Något utrymme för lämplighetsbedömning i det enskilda fallet finns inte. Säkerhetspolisen är skyldig att införa dataskydd som standard oavsett vilken behandling det rör sig om eller vad kostnaderna uppgår till.

4 §

Paragrafen reglerar Säkerhetspolisens skyldighet att säkerställa att det i automatiserade behandlingssystem förs loggar över vissa typer av behandlingar. Övervägandena finns i avsnitt 13.2.3.

En logg är en behandlingshistorik som sparas under en viss tid. Det är en teknisk funktion i systemet som ska fungera automatiskt och som inte ska gå att ändra eller påverka på annat sätt. En logg bör vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Syftet med loggning är dels att verka förebyggande, dels att ge Säkerhetspolisen möjlighet att kontrollera användningen av systemen och att upptäcka felaktig eller obehörig användning av

personuppgifterna. Loggningen bör inte utformas så att den medför onödiga intrång i användarnas integritet.

Krav på loggning vid behandling av personuppgifter följer indirekt av de generella kraven på lämpliga tekniska och organisatoriska åtgärder i både 1 och 7 §§. Förevarande paragraf utgör därmed ett mer preciserat krav på loggning i vissa typer av system. Vad som avses med automatiserade behandlingssystem framgår av kommentaren till 3 §. Standardprogram som Word, Outlook och Excel är i detta sammanhang inte att anse som automatiserade behandlingssystem och omfattas därför inte av kravet på loggning i paragrafen. Inte heller lagringsytor som t.ex. usb-minnen och anställdas personliga mappar på den egna datorn omfattas. Krav på loggning i sådan programvara och på sådana lagringsytor följer dock, i den mån det är tekniskt möjligt, av 1 och 7 §§.

Paragrafen innebär att Säkerhetspolisen ska säkerställa att de automatiserade behandlingssystem som används möjliggör loggning i den utsträckning som krävs och att informationen faktiskt loggas. Av 1 § följer bl.a. krav på logguppföljning. Logguppföljning ska göras systematiskt och återkommande och vara såväl förebyggande som reaktiv. Säkerhetspolisen ska se till att det finns rutiner för logguppföljning.

Paragrafen gäller enligt 14 § även för personuppgiftsbiträden.

Tillgången till personuppgifter

5 §

Paragrafen reglerar den interna tillgången till personuppgifter för dem som arbetar vid Säkerhetspolisen. Övervägandena finns i avsnitt 13.2.4.

Paragrafen innebär att Säkerhetspolisen är skyldig att se till att anställda bara ges tillgång till de personuppgifter som krävs för att de ska kunna fullgöra sina arbetsuppgifter. I Säkerhetspolisens verksamheter behandlas en betydande mängd personuppgifter. De är ofta av integritetskänsligt slag och bör inte spridas till någon som inte är behörig att ta del av uppgifterna. Kravet på behörighetsbegränsning syftar till att minska den interna exponeringen och spridningen av personuppgifterna. Hur det bör göras får bedömas med utgångspunkt i förutsättningarna och Säkerhetspolisens behov. Faktorer som it-systemens storlek och om personuppgifterna är sekretesskyddade eller annars integritetskänsliga ska beaktas.

Paragrafen reglerar inte bara tillgången till Säkerhetspolisens egen information. Vid direktåtkomst är det den mottagande myndigheten som ansvarar för att den egna personalen inte ges tillgång till fler personuppgifter i det it-system som åtkomsten avser än vad arbetsuppgifterna motiverar.

Paragrafen gäller enligt 14 § även för personuppgiftsbiträden.

Konsekvensbedömning och förhandssamråd

6 §

Paragrafen slår fast Säkerhetspolisens skyldighet att inför vissa behandlingar göra en konsekvensbedömning och samråda med tillsynsmyndigheten. Övervägandena finns i avsnitt 13.2.5.

Av *första stycket* framgår att en konsekvensbedömning ska göras om det kan antas att en ny typ av behandling kommer att medföra särskild risk för

intrång i registrerades personliga integritet. En konsekvensbedömning ska också göras om betydande förändringar av redan pågående behandlingar kan antas leda till sådan risk. Vid riskbedömningen bör bl.a. användningen av ny teknik och behandlingens art, omfattning, sammanhang och ändamål beaktas. Exempel på riskfyllda behandlingar som bör föranleda en konsekvensbedömning är inrättandet av storskaliga register som innehåller känsliga personuppgifter eller vissa former av profilering. En konsekvensbedömning ska omfatta relevanta system och processer för behandlingen, men inte behandlingen i enskilda fall.

Andra stycket reglerar s.k. förhandssamråd. När en konsekvensbedömning visar att det finns särskild risk för intrång i registrerades personliga integritet eller när typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten. Samrådet ska äga rum i god tid innan behandlingen påbörjas eller betydande förändringar genomförs. Det bör dock inte äga rum så tidigt att det inte finns något konkret förslag på teknisk lösning för tillsynsmyndigheten att ta ställning till. När förhandssamrådet lämpligen bör äga rum får avgöras i varje enskilt fall och förutsätter en dialog med tillsynsmyndigheten. Tillsynsmyndighetens roll vid förhandssamråd regleras i 7 kap. 1 § 2.

Säkerhetsåtgärder

7 §

I paragrafen regleras Säkerhetspolisens skyldighet att skydda de personuppgifter som behandlas. Övervägandena finns i avsnitt 13.2.7.

Enligt paragrafen ska Säkerhetspolisen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Personuppgifterna ska särskilt skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. Uppräkningen illustrerar vad säkerhetsåtgärderna ska åstadkomma, men den är inte uttömmande.

Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner.

Skydd mot obehörig eller otillåten behandling innebär att obehöriga personer ska vägras åtkomst till utrustning som används vid behandling, att obehörig läsning, kopiering, ändring eller radering av datamedier ska förhindras, att obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter ska förhindras och att obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med uppgiftslämnande eller transport av databärare ska förhindras. Åtgärder ska också vidtas i syfte att säkerställa att personer som är behöriga att använda ett it-system endast har tillgång till personuppgifter som omfattas av deras behörighet. Säkerhetspolisen ska också säkerställa att det kan kontrolleras och fastställas till vilka myndigheter eller andra organ personuppgifter har överförts och för vilka myndigheter eller andra organ uppgifterna har gjorts tillgängliga och att det i efterhand kan kontrolleras och fastställas vilka personuppgifter som förts in i ett it-system, när det har gjorts och av vem.

Skydd mot förlust, förstöring eller annan oavsiktlig skada innebär bl.a. att de it-system som används ska kunna återställas vid störningar, att systemen ska fungera och att funktionsfel rapporteras och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemen.

Vilken skyddsnivå som är lämplig får avgöras från fall till fall. Bedömningen är bl.a. beroende av vilka personuppgifter som behandlas och hur integritetskänsliga de är.

Paragrafen gäller enligt 14 § även för personuppgiftsbiträden.

Samarbete med tillsynsmyndigheten

8 §

I paragrafen regleras Säkerhetspolisens skyldighet att samarbeta med tillsynsmyndigheten. Övervägandena finns i avsnitt 13.2.6. Skyldigheten omfattar enbart samarbete med den myndighet som är tillsynsmyndighet enligt lagen, vilken pekas ut på förordningsnivå. Skyldighet att bistå tillsynsmyndigheten regleras också i 7 kap. 3 §.

Skyldigheten att samarbeta hör samman med tillsynsmyndighetens undersökningsbefogenheter (se 7 kap. 3 §). Skyldigheten innebär inte bara att Säkerhetspolisen ska ge tillsynsmyndigheten tillgång till det material, de resurser och den hjälp som krävs för att den ska kunna utöva tillsyn utan även att myndigheten ska underlätta för tillsynsmyndigheten att utöva sina undersökningsbefogenheter på ett effektivt sätt. Det kan exempelvis innebära att hjälp ska erbjudas och ges inom rimlig tid. Tillsynsmyndigheten ska också ges möjlighet att ta del av information och material på det sätt som den anser mest lämpligt. Tillsynsmyndigheten förutsätts precisera vilken hjälp myndigheten behöver och sätter därigenom ramarna för samarbetsskyldigheten.

Skyldigheten att samarbeta gäller när tillsynsmyndigheten utför sina författningsreglerade uppgifter. Det innebär att bestämmelsen ska tillämpas när tillsynsmyndigheten utövar allmän tillsyn över personuppgiftsbehandling och lämnar råd inom ramen för bl.a. förhandssamråd.

Paragrafen gäller enligt 14 § även för personuppgiftsbiträden.

Dataskyddsombud

9 §

Paragrafen reglerar Säkerhetspolisens skyldighet att utse dataskydds-ombud. Övervägandena finns i avsnitt 13.3.2. Dataskyddsombud definieras i 1 kap. 6 §.

I paragrafen föreskrivs att ett eller flera dataskyddsombud ska utses. Dataskyddsombudet ska vara anställd hos Säkerhetspolisen. Myndigheten får inte utse sig själv till dataskyddsombud. Säkerhetspolisen ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

10 §

I paragrafen anges vilka uppgifter dataskyddsombuden ska utföra. Övervägandena finns i avsnitt 13.3.3.

I *punkt 1* föreskrivs att dataskyddsombuden självständigt ska kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör de skyldigheter som åligger myndigheten som personuppgiftsansvarig. Det innebär att ombuden måste förvissa sig om att Säkerhetspolisen följer bestämmelserna i lagen och andra författningar som reglerar behandlingen av personuppgifter. Hur omfattande kontrollen bör vara får avgöras efter omständigheterna. Dataskyddsombuden bör framför allt granska den faktiska hanteringen av personuppgifter. Därutöver bör ombuden exempelvis granska rutinerna för behandling av personuppgifter, hur tillgången till personuppgifter hanteras och vilka krav på utbildning och andra kvalifikationer som Säkerhetspolisen ställer på personal som behandlar personuppgifter. Ombuden bör påpeka eventuella brister för Säkerhetspolisen så att myndigheten blir medveten om dem och har möjlighet att vidta lämpliga åtgärder.

Kravet på självständighet innebär att dataskyddsombuden ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombudet bör framför allt ha sådan ställning i organisationen att deras synpunkter och råd tas på allvar. De förutsätts också ha goda kunskaper om regelverket om personuppgiftsbehandling.

I *punkt 2* anges att dataskyddsombuden ska informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid sådan behandling. Det handlar främst om att göra Säkerhetspolisen och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att informera registrerade, att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Det innebär inte att dataskyddsombuden ska tala om för Säkerhetspolisen och medarbetarna hur de ska behandla personuppgifter i enskilda fall.

Om Säkerhetspolisen begär det ska dataskyddsombudet också ge råd vid en konsekvensbedömning och kontrollera att bedömningen genomförs på korrekt sätt. Det framgår av *punkt 3*.

Enligt *punkt 4* ska dataskyddsombuden vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter. Syftet med bestämmelsen är att enskilda ska kunna vända sig till en kunnig person inom organisationen i frågor som t.ex. rör information om personuppgiftsbehandlingen och rättelse av felaktiga personuppgifter. Dataskyddsombuden har som kontaktpunkt skyldighet att hjälpa enskilda som vänder sig till myndigheten. I den rollen ligger också att bevaka att Säkerhetspolisen fullgör sina skyldigheter gentemot registrerade. Ombuden behöver däremot inte vidta de åtgärder som kan krävas med anledning av förfrågningar eller klagomål från registrerade.

I *punkt 5* föreskrivs att dataskyddsombuden ska samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter. Samarbeta har här i princip samma innebörd som i 8 §, dvs. det handlar om att underlätta tillsynsmyndighetens arbete. I samarbetsskyldigheten ligger även att ombuden, när det är lämpligt, ska samråda med tillsynsmyndigheten i frågor som rör personuppgiftsbehandling. Det innebär att ombuden vid tveksamheter av olika slag bör fråga tillsynsmyndigheten om råd. Vid förhandssamråd bör arbetsuppgiften

främst bestå i att bistå tillsynsmyndigheten med nödvändigt underlag och information och eventuellt stå till förfogande vid frågor angående behandlingen.

Ett dataskyddsombud behöver inte ägna sig uteslutande åt de arbetsuppgifter som anges i paragrafen. Arbetet som dataskyddsombud kan kombineras med andra arbetsuppgifter, så länge de inte kommer i konflikt med uppdraget som ombud.

Personuppgiftsbiträden

11 §

Av paragrafen framgår att personuppgiftsbiträden får anlitas och vad Säkerhetspolisen måste göra innan ett personuppgiftsbiträde anlitas. Övervägandena finns i avsnitt 13.4.2.

I *första stycket* föreskrivs att Säkerhetspolisen får anlita personuppgiftsbiträden. Det förutsätter dock att det är lämpligt. Om det är lämpligt får avgöras med hänsyn bl.a. till vilka personuppgifter som ska behandlas och om det gäller sekretess för uppgifterna. Av första stycket framgår också att Säkerhetspolisen, innan personuppgiftsbiträdet anlitas, ska försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att personuppgiftsbehandlingen ska vara författningsenlig och för att skydda registrerades rättigheter. Kraven omfattar inte bara säkerhetsåtgärder, utan även andra tekniska och organisatoriska åtgärder. Skyldigheten innebär att Säkerhetspolisen, innan ett personuppgiftsbiträde anlitas, bl.a. bör förhöra sig om hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna kommer att ha.

I *andra stycket* ställs krav på att det ska ingås ett skriftligt avtal eller någon annan skriftlig överenskommelse som reglerar personuppgiftsbiträdets behandling av personuppgifter för Säkerhetspolisens räkning. Eftersom statliga myndigheter, som är att anse som två enheter inom samma juridiska person, i rättslig mening inte kan ingå bindande avtal med varandra får de träffa en skriftlig överenskommelse som reglerar behandlingen.

12 §

Paragrafen reglerar vad som gäller när ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde. Övervägandena finns i avsnitt 13.4.2.

I paragrafen föreskrivs att ett personuppgiftsbiträde inte utan skriftligt tillstånd från Säkerhetspolisen får anlita ett annat personuppgiftsbiträde, ett underbiträde. Ett sådant tillstånd kan gälla biträdets rätt att anlita underbiträden generellt eller i en specifik situation.

13 §

Paragrafen reglerar vad som gäller vid behandling av personuppgifter hos ett personuppgiftsbiträde. Övervägandena finns i avsnitt 13.4.3.

I *första stycket* slås fast den grundläggande principen att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen. Instruktionerna till biträdet bör vara så tydliga att det

inte finns risk för otillåten behandling. Instruktionerna kan exempelvis gälla hur tillgången till personuppgifter hos biträdets anställda ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för dataskydd. Om det finns avvikande regler i annan lagstiftning som föreskriver att personuppgiftsbiträdet är skyldig att utföra viss behandling, t.ex. att lämna ut allmänna handlingar, får behandlingen utföras utan särskilda instruktioner.

I *andra stycket* regleras det fallet där personuppgiftsbiträdet, genom att gå utanför sin befogenhet, behandlar personuppgifter för något annat ändamål än vad som anges i instruktionen. Personuppgiftsbiträdet kan då vara att anse som personuppgiftsansvarig för den behandlingen. Att den som bestämmer ändamålen med och medlen för behandlingen är att anse som personuppgiftsansvarig framgår av definitionen av personuppgiftsansvarig i 1 kap. 6 §. Personuppgiftsbiträdet kan i sådana fall bli skadeståndsskyldig för behandlingen (se 8 kap. 1 §).

14 §

I paragrafen föreskrivs vilka skyldigheter som gäller för personuppgiftsbiträden. Övervägandena finns i avsnitt 13.4.4.

Hänvisningen till 4 och 5 §§ innebär att personuppgiftbiträden, i likhet med Säkerhetspolisen, är skyldiga att dels säkerställa att loggar förs i automatiserade behandlingssystem, dels se till att anställda bara ges tillgång till de personuppgifter som krävs för att fullgöra arbetsuppgifterna. Innebörden av bestämmelserna framgår av kommentarerna till 4 och 5 §§.

Vidare gäller skyldigheten enligt 7 § att vidta lämpliga säkerhetsåtgärder även för personuppgiftsbiträden. Innebörden av skyldigheten framgår av kommentaren till den paragrafen.

Personuppgiftsbiträden är också, genom hänvisningen till 8 §, skyldiga att i samma utsträckning som Säkerhetspolisen samarbeta med tillsynsmyndigheten. Innebörden av skyldigheten framgår av kommentaren till den paragrafen. Personuppgiftsbiträdens skyldighet att samarbeta med tillsynsmyndigheten kan aktualiseras i flera olika situationer. Samarbete kan t.ex. krävas vid tillsyn hos biträdet. Då är samarbetsskyldigheten i princip densamma som för Säkerhetspolisen. Samarbetsskyldigheten kan också aktualiseras vid tillsyn hos Säkerhetspolisen eller inom ramen för Säkerhetspolisens förhandssamråd med tillsynsmyndigheten. Skyldigheten innebär att biträdet också måste samarbeta med Säkerhetspolisen, eftersom det är en förutsättning för att tillsynsmyndigheten ska kunna utföra sitt arbete.

Att personuppgiftsbiträden åläggs vissa skyldigheter fråntar inte Säkerhetspolisen dess ansvar. Säkerhetspolisen är, som framgår av kommentaren till 1 kap. 5 §, ansvarig för den behandling av personuppgifter som personuppgiftsbiträdet utför på myndighetens vägnar. Den omständigheten att personuppgiftsbiträden ges en direkt skyldighet att vidta vissa åtgärder innebär dock att tillsynsmyndigheten vid brister kan vidta åtgärder mot både personuppgiftsbiträdet och Säkerhetspolisen.

Kap 6. Enskildas rättigheter

Rätten till information

Allmän information

1 §

I paragrafen anges vilken allmän information som Säkerhetspolisen på eget initiativ ska göra tillgänglig för registrerade. Informationen, som riktar sig till allmänheten eller en obestämd, större krets av registrerade, kan göras tillgänglig t.ex. på myndighetens webbplats. Övervägandena finns i avsnitt 14.2.1.

Enligt *punkt 1* ska myndighetens identitet och kontaktuppgifter göras tillgängliga. Med det avses uppgifter om namn, post- och besöksadress, telefonnummer och e-postadress.

Enligt *punkt 2* ska dataskyddsombudets kontaktuppgifter anges. Säkerhetspolisen är enligt 5 kap. 9 § skyldig att utse dataskyddsombud. Det behöver inte vara en kontaktuppgift direkt till dataskyddsombudet, t.ex. hans eller hennes e-postadress, utan det är tillräckligt att ombudet går att nå med hjälp av uppgifterna.

I *punkt 3* föreskrivs att kategorier av ändamål för behandlingen ska framgå. Det är alltså inte ändamålen med behandlingen av personuppgifter i enskilda fall som avses utan vilka kategorier av ändamål som Säkerhetspolisen behandlar personuppgifter för. Det kan t.ex. vara förundersökning, underrättelsearbete och åtgärder inom ett särskilt verksamhetsområde, t.ex. kontraterrorism, eller åtgärder som vidtas inom ramen för säkerhetsskyddsarbetet, exempelvis säkerhetsprövning och registerkontroll.

I *punkt 4* och *5* föreskrivs att Säkerhetspolisen ska upplysa om de rättigheter som enskilda har enligt 2, 6 och 7 §§. Det gäller rätten för registrerade att få information om behandlingen av personuppgifter och att få del av uppgifterna och rätten att begära rättelse, radering eller begränsning av behandlingen.

Personrelaterad information

2 §

I paragrafen regleras vilken information som ska lämnas på begäran av en enskild. Övervägandena finns i avsnitt 14.2.2.

I *första stycket* föreskrivs att den som begär det har rätt till skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och få viss i paragrafen uppräknad skriftlig information.

Vem som helst får begära besked av Säkerhetspolisen. Vårdnadshavare och andra ställföreträdare kan begära besked för den som inte själv har rätt att göra det. Om en underårig förstår vad åtgärden innebär och själv kan tillgodogöra sig den information som begäran avser bör hans eller hennes begäran godtas. Sökanden har bevisbördan för att begäran har gjorts och tidpunkten för det. Bestämmelsen i 22 § förvaltningslagen (2017:900) kan vara till ledning vid avgörande av frågan om när en begäran ska anses ha gjorts (jfr prop. 1997/98:44 s. 132). Begäran ska besvaras utan onödigt dröjsmål. Beskedet till sökanden ska vara skriftligt och kan lämnas t.ex. via e-post. Det ska avse om personuppgifter som rör sökanden behandlas.

Om sökandens personuppgifter behandlas ska, med de begränsningar som följer av andra stycket och 3–5 §§, han eller hon få del av dem. Rätten omfattar även personuppgifter som utgörs av bild- och ljudupptagningar och personuppgifter i ostrukturerat material som t.ex. löpande text.

Det är de uppgifter som behandlas vid tiden för utlämnandet som ska lämnas ut (jfr prop. 1997/98:44 s. 132). Sökanden ska få tillgång till all information som Säkerhetspolisen själv kan få fram om honom eller henne, men det är tillräckligt att använda de sök- och sammanställningsmöjligheter som är faktiskt tillgängliga och rättsligt tillåtna (jfr prop. 1997/98:44 s. 82 f.). Det bör räcka att sökningar görs i myndighetens verksamhetsspecifika behandlingssystem, t.ex. dokument- och ärendehanteringssystem, register och databaser. Om uppgifter är sökbara i standardprogram som Word, Outlook och Excel bör de också omfattas.

För att det ska kunna utrönas om personuppgifter behandlas krävs att det finns sökbara uppgifter som direkt kan hänföras till den person som begär informationen. Sökanden förutsätts därför lämna sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen. Det kan t.ex. vara fullständigt namn eller person- eller samordningsnummer.

Sökanden kan få del av uppgifterna genom t.ex. en kopia av en handling med de personuppgifter som rör honom eller henne. Säkerhetspolisen har dock ingen skyldighet att lämna ut en kopia om sökandens rättigheter kan säkerställas på annat sätt, t.ex. genom en sammanfattning av vilka personuppgifter som behandlas.

Sökanden ska också informeras om behandlingen av personuppgifterna. Enligt *punkt 1* och *2* ska informationen avse vilka personuppgifter om sökanden som behandlas och, om det är känt, varifrån uppgifterna kommer.

I *punkt 3* föreskrivs att den rättsliga grunden för behandlingen ska anges. Den rättsliga grunden kan t.ex. vara att det är nödvändigt att behandla personuppgifterna vid utredning av ett terrorbrott eller för att fullgöra uppgifter enligt säkerhetsskyddslagen (se 2 kap. 1 §).

Vidare ska enligt *punkt 4* information om ändamålen med behandlingen lämnas. Det som avses är ändamålen i det enskilda fallet, t.ex. vilket ärende eller vilken förundersökning det är fråga om.

Enligt *punkt 5* ska information om mottagare eller kategorier av mottagare av personuppgifterna lämnas. Mottagare definieras i 1 kap. 6 §. Allmän information är tillräcklig, exempelvis till vilken typ av myndighet som personuppgifterna har lämnats eller ska lämnas. Det kan vara t.ex. allmän domstol. Om mottagarkategorin finns i ett tredjeland eller är en internationell organisation ska det anges.

Enligt *punkt 6* ska information också lämnas om hur länge personuppgifterna får behandlas. Om det inte är möjligt att ange hur länge uppgifterna får behandlas i det enskilda fallet ska i stället kriterierna för att fastställa det anges. Det kan vara upplysningar om vilka omständigheter eller tidpunkter som styr hur länge uppgifterna får behandlas, t.ex. nedläggning av åtal eller när viss tid förflutit efter det att uppgifterna behandlades för första gången.

I *punkt 7* föreskrivs att den personuppgiftsansvarige ska informera om rätten att begära rättelse, radering eller begränsning av behandlingen.

I *andra stycket* begränsas rätten att få del av personuppgifter. Om sökanden redan har tagit del av personuppgifterna behöver de inte lämnas

ut till honom eller henne. Det har ingen betydelse på vilket sätt sökanden fått del av dem. Det kan t.ex. vara personuppgifter i handlingar som sökanden själv har skickat in till myndigheten eller som Säkerhetspolisen har expedierat till honom eller henne. Säkerhetspolisen måste emellertid tydligt ange vilka personuppgifter som behandlas och ge sökanden en förteckning över dem. Vidare har sökanden rätt att få del av personuppgifterna om han eller hon begär det. Om en begäran om information är orimlig eller uppenbart ogrundad får den avslås enligt 5 § första stycket.

I 9 § föreskrivs att information enligt förevarande paragraf ska lämnas till den registrerade avgiftsfritt en gång per år och att utlämnande därutöver kan avgiftsbeläggas.

Begränsning av rätten till information

3 §

Paragrafen gör undantag från Säkerhetspolisens informationsskyldighet. Övervägandena finns i avsnitt 14.3.1.

Enligt *första stycket* gäller Säkerhetspolisens skyldighet att lämna personrelaterad information enligt 2 § inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifterna inte får lämnas ut. Regleringen innebär att Säkerhetspolisen får begränsa eller utelämna informationen. Det är främst sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen (2009:400) som avses. Även andra bestämmelser om tystnadsplikt och bestämmelser som begränsar möjligheten att använda uppgifter som Säkerhetspolisen har fått från en myndighet i en annan stat kan begränsa informationsskyldigheten. Undantaget från informationsskyldigheten gäller även vid beslut som har meddelats med stöd av författning, t.ex. beslut om förbehåll enligt 10 kap. 14 § offentlighets- och sekretesslagen.

Säkerhetspolisen är enligt *andra stycket* inte heller skyldig att lämna ut skälen för beslut enligt första stycket eller skälen för beslut i fråga om rättelse, radering eller begränsning av behandlingen, om motiveringen skulle riskera att skada något av de intressen som sekretessen eller tystnadsplikten avser att skydda.

4 §

Paragrafen föreskriver undantag från informationsskyldigheten i 2 § för personuppgifter i viss typ av text. Övervägandena finns i avsnitt 14.3.2.

Säkerhetspolisen skyldighet att lämna personrelaterad information enligt 2 § gäller enligt *första stycket* inte för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller text som utgör minnesanteckningar eller liknande. Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas. Bild- och ljudupptagningar omfattas inte av undantaget eftersom det bara gäller text. Med text som inte fått sin slutliga utformning avses koncept eller utkast till protokoll, skrivelser, beslut eller liknande. Löpande text som är avsedd att tidvis ändras eller kompletteras och därför aldrig får någon slutlig utformning omfattas inte. Det sistnämnda kan t.ex.

vara diarier, journaler, register eller förteckningar som förs löpande. Med minnesanteckning avses anteckningar som utgör hjälpmedel för handläggningen, t.ex. promemorior och andra anteckningar eller upptagningar som har skapats bara för att förbereda ett ärende för avgörande och som inte har tillfört ärendet något i sak.

Av *andra stycket* framgår att undantaget från informationsskyldigheten inte gäller under vissa förhållanden. Sökanden har då rätt att få del av personuppgifter även i löpande text som inte fått sin slutliga utformning eller i minnesanteckningar och liknande.

Enligt *punkt 1* gäller undantaget inte om personuppgifterna har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Tredje man definieras i 1 kap. 6 §. Det är den version av uppgifterna i t.ex. utkastet som lämnades till tredje man som informationsskyldigheten omfattar, även om utkastet därefter har ändrats.

Enligt *punkt 2* gäller undantaget inte om personuppgifterna behandlas enbart för vetenskapliga, statistiska eller historiska ändamål. Om ett utkast eller en minnesanteckning endast används vid statistikproduktion eller för vetenskapliga eller historiska ändamål inom lagens tillämpningsområde ska alltså information om behandlingen av personuppgifterna lämnas ut.

I *punkt 3* anges att undantaget inte heller gäller för personuppgifter som har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Det är tidpunkten för begäran som är avgörande för bedömningen av om något av undantagen gäller. Både ettårsfristen och frågan om uppgifterna har lämnats ut till tredje man eller behandlas för vetenskapliga, statistiska eller historiska ändamål ska bedömas i förhållande till när begäran om information gjordes (jfr prop. 1997/98:44 s. 83 f.).

5 §

Paragrafen föreskriver att information enligt 2 § inte behöver lämnas om begäran är orimlig eller uppenbart ogrundad. Övervägandena finns i avsnitt 14.3.3.

I *första stycket* föreskrivs att Säkerhetspolisen får avslå en begäran att få information om behandlingen av personuppgifter och få del av dem om begäran är orimlig eller uppenbart ogrundad. En begäran kan vara orimlig t.ex. om den upprepas ofta. En begäran kan också vara orimlig om den är så oprecis att det skulle vara närmast omöjligt att besvara den, t.ex. om den rör hela verksamheten. Normalt bör i sådana fall begäran kunna preciseras till viss verksamhet, visst ärende eller någon annan liknande avgränsning. En begäran kan vara uppenbart ogrundad t.ex. om sökanden missbrukar sin rätt till information genom att exempelvis lämna felaktiga eller missvisande uppgifter i sin begäran. Säkerhetspolisen har bevisbördan för att en begäran är orimlig eller uppenbart ogrundad.

I *andra stycket* upplyses att Säkerhetspolisen, med stöd av 9 § andra stycket, i vissa fall får ta ut avgift i stället för att avslå begäran.

Rätten till rättelse, radering och begränsning av behandlingen

6 §

Paragrafen reglerar den enskildes rätt att begära rättelse eller komplettering av felaktiga eller ofullständiga personuppgifter och begränsning av behandlingen av personuppgifterna. Övervägandena finns i avsnitt 14.4.1 och 14.4.3. I 2 kap. 13 § regleras Säkerhetspolisens skyldighet att på eget initiativ rätta felaktiga eller ofullständiga personuppgifter och uppdatera inaktuella personuppgifter.

Enligt *första stycket* ska Säkerhetspolisen på begäran av den registrerade rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Vårdnadshavare och andra ställföreträdare kan begära rättelse eller komplettering åt en registrerad som inte själv har rätt att göra det. I kommentaren till 2 kap. 7 § framgår vad som avses med att en personuppgift är korrekt och vilka bedömningar som ska göras.

Rättelse eller komplettering ska göras utan onödigt dröjsmål. Det innebär att Säkerhetspolisen skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt genomföra åtgärden.

Säkerhetspolisen ska enligt *andra stycket* begränsa behandlingen av personuppgifter som rör den registrerade om han eller hon ifrågasätter att de är korrekta. Den registrerade kan ha en annan uppfattning än Säkerhetspolisen om huruvida en personuppgift är korrekt. Om korrektheten ifrågasätts är myndigheten skyldig att försöka klarlägga hur det förhåller sig. Om Säkerhetspolisens utredning om den omstridda personuppgiften inte kan slutföras inom den tid som en personuppgift ska rättas eller kompletteras, ska behandlingen begränsas under utredningstiden.

Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av vare sig Säkerhetspolisen, ett personuppgiftsbiträde eller någon annan, utom för de ändamål för vilka behandlingen begränsades. Uppgiften får dock lämnas ut med stöd av 2 kap. tryckfrihetsförordningen. Säkerhetspolisen ska vidta åtgärder som visar att behandlingen av personuppgiften har begränsats. En sådan åtgärd kan vara att föra över uppgiften från det datasystem där den behandlas, t.ex. myndighetens verksamhetssystem, till ett arkivsystem. Andra åtgärder kan vara att göra personuppgiften oåtkomlig genom en teknisk begränsning eller annan inskränkning av tillgången till uppgiften. När utredningen om personuppgiften är avslutad ska begränsningen av behandlingen upphöra. Då ska personuppgiften antingen rättas eller fortsätta att behandlas som tidigare.

7 §

Paragrafen reglerar den enskildes rätt att vid otillåten behandling av personuppgifter begära radering eller, om personuppgifterna behöver finnas kvar av bevisskäl, begränsning av behandlingen. Övervägandena finns i avsnitt 14.4.2 och 14.4.3. I 2 kap. 14 § regleras Säkerhetspolisen skyldighet att på eget initiativ radera eller begränsa behandlingen av personuppgifter som behandlas på otillåtet sätt.

Enligt *första stycket* ska Säkerhetspolisen på begäran av den registrerade radera personuppgifter som rör honom eller henne, om de behandlas i strid

med 2 kap. 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–10 §, eller om det krävs för att Säkerhetspolisen ska utföra en rättslig förpliktelse. Vårdnadshavare och andra ställföreträdare kan begära radering för en registrerad som inte har rätt att själv göra det.

Om personuppgifter behandlas i strid med någon av de bestämmelser som räknas upp i paragrafen ska de på begäran av den registrerade raderas. Med radering avses att personuppgifter tas bort från informationssamlingar på ett sådant sätt att de inte längre kan återskapas. I de aktuella bestämmelserna föreskrivs bl.a. att personuppgifter ska vara adekvata och relevanta, att inte fler personuppgifter än nödvändigt får behandlas och att de bara får behandlas om det finns en rättslig grund och för särskilt angivna ändamål. Där regleras också behandling av känsliga personuppgifter och hur länge personuppgifter får behandlas. Frågan om en personuppgift ska raderas ska bedömas mot bakgrund av kraven i dessa bestämmelser.

Personuppgifter ska också raderas på begäran av den registrerade om det krävs för att Säkerhetspolisen ska utföra en rättslig förpliktelse. Rättslig förpliktelse kan avse en skyldighet som rör hur personuppgifter får behandlas enligt denna lag eller annan författning, t.ex. lagen (1998:621) om misstankeregister.

Utrymmet för att radera uppgifter i allmänna handlingar begränsas av arkivlagstiftningen genom att det krävs författningsstöd för gallring.

Radering ska göras utan onödigt dröjsmål. Det innebär att Säkerhetspolisen skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt radera uppgiften.

Om förutsättningarna för att radera personuppgifterna är uppfyllda, men uppgifterna behöver finnas kvar av bevisskäl, ska Säkerhetspolisen enligt *andra stycket* på begäran av den registrerade i stället begränsa behandlingen av uppgifterna.

En begränsning kan bara göras i de fall där personuppgifterna behandlas otillåtet, eftersom det endast är då som radering kan komma i fråga. För att personuppgifterna inte ska raderas ska de behövas som bevisning, t.ex. i en rättsprocess angående otillåten personuppgiftsbehandling. Däremot är det inte tillåtet att ha kvar personuppgifter som ska raderas i syfte att använda dem t.ex. för brottsbekämpning.

Begränsning av behandlingen är inte en permanent åtgärd. När personuppgifterna inte längre behöver finnas kvar av bevisskäl, t.ex. för att domen eller beslutet i skadeståndsmålet har fått laga kraft, ska begränsningen upphöra och personuppgifterna raderas.

Behandlingen ska begränsas utan onödigt dröjsmål. Hur det kan göras utvecklas i kommentaren till 6 §.

8 §

Enligt paragrafen avgör Säkerhetspolisen vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen. Övervägandena finns i avsnitt 14.4.4.

Paragrafen innebär att Säkerhetspolisen – med beaktande av vilken åtgärd som är lagligen möjlig att vidta – ska se till att den lämpligaste åtgärden vidtas oavsett vilken åtgärd som begärs av den registrerade. Vad som är mest lämpligt ska bedömas med utgångspunkt i både

verksamhetens behov och den registrerades rätt till skydd för sina personuppgifter.

Avgiftsfri information

9 §

Paragrafen föreskriver att information som huvudregel ska vara avgiftsfri. Övervägandena finns i avsnitt 14.3.3 och 14.5.

I *första stycket* slås fast att den information som Säkerhetspolisen på eget initiativ ska göra tillgänglig för registrerade ska vara avgiftsfri, medan den information om behandlingen av den registrerades personuppgifter som lämnas på begäran ska vara avgiftsfri en gång per år.

I *andra stycket* föreskrivs att om någon begär att få information om behandlingen av personuppgifter och få del av dem oftare än en gång per år får Säkerhetspolisen ta ut en rimlig avgift för det. Myndigheten får, i stället för att ta ut avgift, avslå begäran, vilket regleras i 5 § första stycket. Utgångspunkten bör vara att Säkerhetspolisen i första hand tar ut avgift och i andra hand avslår begäran om information. Vilken åtgärd som är lämpligast får avgöras med utgångspunkt i omständigheterna i det enskilda fallet. En viktig faktor är hur många framställningar om information som personen har gjort under året och hur lång tid som förflutit efter den senaste framställan. Även omständigheter som hur preciserad eller komplicerad begäran är och vilka skäl han eller hon anger för sin begäran bör beaktas.

Om Säkerhetspolisen avser att ta ut avgift bör den som begärt informationen underrättas om det. Myndigheten bör förhöra sig om begäran vidhålls. Avgiften ska vara rimlig, vilket innebär att den inte får överstiga de administrativa kostnaderna för att besvara begäran.

7 kap. Tillsyn

Tillsynsmyndighetens uppgifter

1 §

Paragrafen reglerar tillsynsmyndighetens uppgifter. Överväganden finns i avsnitt 15.4.

I paragrafen anges de huvudsakliga tillsynsuppgifterna. Tillsynsmyndigheten avgör i vilken utsträckning tillsyn ska utövas och hur den ska genomföras. Myndigheten ska agera helt oberoende vid denna bedömning. Det innebär att ingen kan kräva att myndigheten ska utöva tillsyn. Det finns inte heller några formella krav på hur tillsynen ska utövas, med undantag från vissa bestämmelser i denna lag och i föreskrifter som beslutas i anslutning till den. Om tillsynsmyndigheten beslutar att inleda ett tillsynsärende tillämpas förvaltningslagen (2017:900) på handläggningen om det inte finns avvikande bestämmelser (se avsnitt 15.6).

I *punkt 1* anges tillsynsmyndighetens allmänna uppgift att utöva tillsyn över behandlingen av personuppgifter. Vad det innebär utvecklas i avsnitt 15.4.1.

I *punkt 2* regleras tillsynsmyndighetens skyldighet att lämna råd och stöd till Säkerhetspolisen och till personuppgiftsbiträden. Med råd avses både muntliga och skriftliga råd. Det kan vara fråga om allmänna råd eller

rådgivning i ett enskilt fall. Det kan även vara fråga om rådgivning vid förhandssamråd enligt 5 kap. 6 §. Rådgivning av sistnämnda slag är tillsynsmyndigheten skyldig att bistå med, medan myndigheten i övrigt ska ge råd och stöd bara när den anser att det är påkallat. Rådgivningen och stödet ska avse Säkerhetspolisens och personuppgiftsbiträdens allmänna skyldigheter.

Råd kan t.ex. lämnas genom information på tillsynsmyndighetens hemsida, genom publicering av allmänna råd eller andra riktlinjer eller någon funktion för rådgivning per telefon eller e-post. Paragrafen ger således ingen rätt för Säkerhetspolisen eller personuppgiftsbiträden att avkräva tillsynsmyndigheten råd i en konkret fråga, om det inte är särskilt reglerat. Förhandssamråd är exempel på det sistnämnda.

2 §

Paragrafen upplyser om att bestämmelser om tillsyn över Säkerhetspolisens personuppgiftsbehandling även finns i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Paragrafen behandlas i avsnitt 15.3.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

3 §

Paragrafen reglerar tillsynsmyndighetens undersökningsbefogenheter. Övervägandena finns i avsnitt 15.5.1.

Enligt *punkt 1* har tillsynsmyndigheten rätt att för sin tillsyn från Säkerhetspolisen och personuppgiftsbiträden få tillgång till alla personuppgifter som behandlas. Det innebär att Säkerhetspolisen ska lämna de begärda uppgifterna även om det kräver viss efterforskning.

Punkt 2 ger tillsynsmyndigheten rätt till upplysningar och dokumentation som rör behandlingen av personuppgifter och vilka åtgärder som har vidtagits för att säkerställa skyddet för personuppgifterna och registrerades personliga integritet. Dokumentationen kan avse exempelvis loggar som Säkerhetspolisen och personuppgiftsbiträden ska föra. Det kan också vara fråga om upplysningar om och dokumentation av vilka organisatoriska och tekniska åtgärder som vidtogs i samband med att ett register inrättades eller en viss typ av behandling påbörjades. Det kan vidare röra sig om åtgärder för att garantera säkerheten, begränsa den interna tillgången till uppgifter eller förhindra otillåten behandling och åtgärder för intern kontroll. Informationen kan avse exempelvis ändamålen med behandlingen eller loggar och förteckningar över pågående behandlingar. Att en myndighet saknar faktisk möjlighet att påverka hur uppgifter hanteras innan de blir tillgängliga hos myndigheten hindrar inte att den är skyldig att redovisa säkerheten vid behandlingen (se HFD 2012 ref. 21).

I *punkt 3* regleras tillsynsmyndighetens rätt att få tillträde till lokaler som Säkerhetspolisen eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel som används för behandlingen. Rätten till tillträde ger inte myndigheten rätt att bereda sig tillträde med tvång. Om Säkerhetspolisen eller personuppgiftsbiträdet inte samarbetar kan tillsynsmyndigheten utnyttja sina korrigerande befogenheter enligt 5 §.

Tillsynsmyndigheten har också rätt att få tillgång till den utrustning som tillsynsobjektet disponerar för att, med hjälp av tillsynsobjektets personal, kunna göra nödvändiga körningar och kontroller. Punkten ger således inte tillsynsmyndigheten någon rätt att fritt använda tillsynsobjektets utrustning och datasystem.

Punkt 4 klargör att tillsynsmyndigheten har rätt att få hjälp med de sökningar och andra åtgärder som den begär och annan nödvändig hjälp för att genomföra tillsynen. Punkten ger även tillsynsmyndigheten rätt till information som inte har direkt anknytning till behandlingen av personuppgifter, men som myndigheten behöver för tillsynen. Informationen kan avse t.ex. verksamhetsplaner som beskriver den verksamhet där behandlingen utförs.

Tillsynsmyndighetens tillgång till information och lokaler är underkastat de begränsningar som följer av t.ex. säkerhetsskyddslagen (2018:585) i fråga om bl.a. krav på säkerhetsprövning av tillsynsmyndighetens personal.

Förebyggande befogenheter

4 §

Paragrafen reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. De åtgärder som regleras i paragrafen är inte av tvingande karaktär. De syftar till att förebygga att framtida behandling av personuppgifter står i strid med regelverket. Övervägandena finns i avsnitt 15.5.3.

Av *första stycket* framgår att tillsynsmyndigheten, om det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att motverka risken genom råd, rekommendationer och påpekanden. Det kan vara fråga om ett nytt register som ska inrättas, en ny typ av behandling som ska påbörjas eller en större förändring av pågående behandling. Tillsynsmyndigheten kan också identifiera risker i pågående behandling som skulle kunna innebära att regelverket inte kommer att följas. Rådgivning kan avse såväl formella som informella samråd. Av 5 § första stycket 1 framgår att de befogenheter som räknas upp i detta stycke även i vissa fall får användas i korrigerande syfte.

Enligt *andra stycket* får tillsynsmyndigheten skriftligen varna för att viss behandling riskerar att strida mot regelverket. En varning är en mer ingripande åtgärd än åtgärderna i första stycket. Varning kan användas för att visa hur allvarligt tillsynsmyndigheten ser på den planerade behandlingen. Tillsynsmyndigheten behöver inte ha uttömt andra förebyggande åtgärder innan den utfärdar en varning. En varning ska vara skriftlig. Av den ska framgå varför tillsynsmyndigheten bedömt att behandlingen inte kommer att vara författningsenlig. Åtgärden är inte tvingande, men den som får en varning förväntas rätta sig efter den.

Varning får också utfärdas om pågående behandling riskerar att stå i strid med lag eller annan författning. Det kan t.ex. aktualiseras om det vid förhandssamråd enligt 5 kap. 6 § andra stycket visar sig att det finns risk för att de förändringar som planeras kan göra att den framtida behandlingen inte blir författningsenlig.

Korrigerande befogenheter

5 §

I paragrafen regleras tillsynsmyndighetens korrigerande befogenheter. Övervägandena finns i avsnitt 15.5.4.

Tillsynsmyndigheten har möjlighet att successivt använda olika medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig. Förutom de medel som anges i första stycket 1 är befogenheterna tvingande. Befogenheterna anges i stegrande ordning, men är inte kopplade till varandra på det sättet att en strängare åtgärd förutsätter att mindre ingripande åtgärder redan har prövats.

De korrigerande befogenheterna får användas när tillsynsmyndigheten konstaterar att Säkerhetspolisen behandlar personuppgifter i strid med lag eller annan författning eller på något annat sätt inte fullgör sina skyldigheter. De skyldigheter som avses är framför allt skyldigheterna i 5 kap. Säkerhetspolisen har emellertid också skyldigheter enligt 6 och 9 kap. och skyldighet att bistå tillsynsmyndigheten enligt 3 §. Även underlåtenhet att fullgöra sådana skyldigheter och skyldigheter som regleras i föreskrifter med anledning av denna lag omfattas.

Enligt *första stycket punkt 1* får tillsynsmyndigheten använda de förebyggande befogenheter som regleras i 4 § första stycket för att försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter. Vilka befogenheter tillsynsmyndigheten kan använda utvecklas i kommentaren till 4 §. Vad som avses med författningsenlig utvecklas i kommentaren till 2 kap. 6 §.

Enligt *punkt 2* får tillsynsmyndigheten förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att viss behandling av personuppgifter ska bli författningsenlig eller för att de ska uppfylla andra skyldigheter. Sådana förelägganden är bindande för mottagaren. Tillsynsmyndigheten kan t.ex. förelägga Säkerhetspolisen att förändra viss personuppgiftsbehandling eller att uppfylla krav på loggning eller dokumentationsskyldighet. Ett föreläggande kan också avse att myndigheten ska rätta, komplettera eller radera en personuppgift. Tillsynsmyndigheten kan även förelägga Säkerhetspolisen att vidta ytterligare tekniska eller organisatoriska åtgärder för säkerheten vid behandling eller att inrätta en intern ordning för anmälan av överträdelser av bestämmelserna, upprätta konsekvensbedömning eller fullgöra samrådsskyldighet.

Punkt 3 ger tillsynsmyndigheten rätt att förbjuda fortsatt behandling, om Säkerhetspolisen eller biträdet allvarligt brister i sina skyldigheter. Med förbud mot fortsatt behandling avses att uppgifter inte längre får behandlas för de ändamål som Säkerhetspolisen har bestämt, utan endast får behandlas i syfte att uppfylla 2 kap. tryckfrihetsförordningen. För förbud bör krävas, förutom att det är fråga om allvarliga brister, att bristerna i fråga inte kan avhjälpas genom andra mindre ingripande åtgärder. En sådan allvarlig brist kan vara att personuppgifter behandlas för ändamål som inte är tillåtna. Att tillsynsmyndigheten inte på begäran får det underlag eller den hjälp som den har rätt till enligt 3 § kan i vissa fall vara en allvarlig brist, t.ex. att myndigheten vägras tillträde. Det kan också vara

en allvarlig brist om Säkerhetspolisen eller personuppgiftsbiträdet inte rättar sig efter ett föreläggande eller negligerar en skriftlig varning.

Ett förbud enligt punkt 3 kan vara permanent. Tillsynsmyndigheten kan också meddela ett tillfälligt förbud om den anser att det finns förutsättningar för att bristen, trots att den är allvarlig, ska kunna åtgärdas.

Det ankommer på Säkerhetspolisen eller personuppgiftsbiträdet att vidta de tekniska åtgärder som krävs för att personuppgifterna inte längre ska kunna behandlas om fortsatt behandling förbjuds.

Beslut enligt första stycket punkterna 2 och 3 ska vara skriftliga och motiveras. Tillsynsmyndighetens beslut gäller först efter att de har fått laga kraft (jfr 6 §). Besluten kan överklagas enligt 8 kap. 3 §.

I *andra stycket* föreskrivs att det av ett föreläggande alltid ska framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas. Om föreläggandet avser rättelse, komplettering, radering eller begränsning av behandlingen bör det framgå av föreläggandet vad som ska göras. Tillsynsmyndigheten får emellertid överlåta åt Säkerhetspolisen att avgöra vilka åtgärder som ska vidtas för att behandlingen ska bli författningsenlig eller hur andra skyldigheter ska fullgöras. Det kan vara lämpligt när det är fråga om tekniska eller organisatoriska åtgärder som ska vidtas eller när det annars finns olika alternativ för vilka åtgärder som kan vidtas och hur de bör genomföras.

Verkställighet av beslut

6 §

Paragrafen reglerar när tillsynsmyndighetens beslut kan verkställas. Övervägandena finns i avsnitt 15.6.3.

Paragrafen innebär ett undantag från förvaltningslagens bestämmelser om verkställighet. Tillsynsmyndighetens beslut ska endast kunna verkställas efter att de har fått laga kraft. Bestämmelsen innebär att förvaltningslagens möjligheter att i vissa fall göra undantag från huvudregeln om att laga kraft är en förutsättning för verkställighet, inte gäller för tillsynsmyndighetens beslut.

8 kap. Skadestånd och överklagande

Skadestånd

1 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Övervägandena finns i avsnitt 16.3.2.

Paragrafen är en sådan specialbestämmelse om skadestånd som enligt 1 kap. 1 § skadeståndslagen (1972:207) tar över reglerna i den lagen. Om en ersättningsfråga inte berörs i paragrafen – t.ex. frågan om hur ersättningen för en personskada eller sakskada ska beräknas (5 kap. skadeståndslagen) eller hur ansvaret ska fördelas när flera är skadeståndsskyldiga (6 kap. 4 § skadeståndslagen) – tillämpas de allmänna reglerna i skadeståndslagen.

Rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i denna lag eller föreskrifter som meddelats i anslutning till

lagen. För att den personuppgiftsansvarige ska bli ersättningsskyldig behöver den registrerade bevisa att behandling av hans eller hennes personuppgifter stått i strid med reglerna om personuppgiftsbehandling och att den har skadat eller kränkt honom eller henne.

Den registrerades rätt till skadestånd omfattar ersättning för skada och för kränkning av den personliga integriteten. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom behandlingen.

Det är bara sådan skada eller kränkning som behandlingen av personuppgifter har vållat som ersätts, vilket framgår av att behandlingen ska ha orsakat skada respektive kränkning. Orsakssambandet ska vara adekvat. Ersättningen för kränkning får uppskattas efter skälighet mot bakgrund av samtliga omständigheter i det enskilda fallet. Sådana faktorer som att det funnits risk för otillbörlig spridning av känsliga eller felaktiga personuppgifter eller att den registrerade genom behandlingen av uppgifterna drabbats av beslut eller åtgärder som kunnat få negativa följder, hör till det som bör beaktas. Har den registrerade själv lämnat en oriktig eller ofullständig personuppgift, kan även detta ha betydelse vid bedömningen.

Gentemot den registrerade är Säkerhetspolisen ansvarig för all den behandling som utförs för myndighetens räkning. Det gäller även när ett personuppgiftsbiträde eller någon annan utfört behandlingen. Anspråk på skadestånd ska således riktas mot Säkerhetspolisen även i de fallen. Personuppgiftsbiträdet kan dock ibland vara att anse som personuppgiftsansvarig för viss behandling och kan då bli skadeståndsskyldig i den egenskapen.

Paragrafen innehåller ingen bestämmelse som innebär att ersättningsskyldigheten kan jämkas. Det torde dock finnas utrymme för att sätta ned skadestånd med stöd av allmänna skadeståndsrättsliga principer om jämkning.

Överklagande

Överklagande av den personuppgiftsansvariges beslut

2 §

I paragrafen anges i vilken utsträckning beslut som fattats av den personuppgiftsansvarige får överklagas till allmän förvaltningsdomstol. Övervägandena finns i avsnitt 16.4.

Vilka typer av beslut som får överklagas räknas upp i *första stycket*. Uppräkningen är, som framgår av 4 §, uttömmande. Beslut i fråga om rättelse, komplettering eller radering av personuppgifter eller begränsning av behandlingen av personuppgifter får överklagas om den registrerade har begärt åtgärden och beslutet har gått honom eller henne emot. Rätten att överklaga kan gälla även i de fall den personuppgiftsansvarige vidtagit en annan åtgärd än den som den registrerade begärt.

Beslut som innebär att en begäran om personrelaterad information, helt eller delvis, inte har tillmötesgåtts får också överklagas. Detsamma gäller beslut att ta ut avgift för viss information.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 §

I paragrafen föreskrivs att tillsynsmyndighetens beslut enligt lagen får överklagas till allmän förvaltningsdomstol. Övervägandena finns i avsnitt 16.4.2.

Utgångspunkten enligt *första stycket* är att tillsynsmyndighetens beslut enligt lagen får överklagas. Det är framför allt fråga om beslut som tillsynsmyndigheten har fattat med stöd av sina korrigerande befogenheter i 7 kap. 5 §. Det kan t.ex. vara beslut om rättelse eller radering. I stycket anges vidare att tillsynsmyndigheten är motpart i domstolen när ett beslut överklagas.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagandeförbud

4 §

Enligt paragrafen får inga andra beslut än de som räknas upp i 2 och 3 §§ överklagas. Övervägandena finns i avsnitt 16.4.

Uppräkningen är uttömmande. Någon rätt att med stöd av förvaltningslagen (2017:900) överklaga andra beslut som Säkerhetspolisen eller annan har fattat med stöd av lagen finns alltså inte.

9 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för överföring

1 §

I paragrafen anges förutsättningarna för att få överföra personuppgifter till ett tredjeland eller en internationell organisation. Övervägandena finns i avsnitt 17.3.

Enligt *första stycket* får Säkerhetspolisen överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Tredjeland och internationell organisation definieras i 1 kap. 6 §.

Med behandlas förstås sådan behandling av personuppgifter som lagen reglerar. Behandling av personuppgifter definieras i 1 kap. 6 §. Överföring är en form av personuppgiftsbehandling. För att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation måste därför de allmänna förutsättningarna för att få behandla personuppgifter i 2 kap. alltid vara uppfyllda, exempelvis kraven på ändamål och personuppgifternas kvalitet.

Med överföring avses att Säkerhetspolisen skickar, vidarebefordrar eller förmedlar information till någon som befinner sig i ett tredjeland eller till en internationell organisation. Det har inte någon betydelse om

överföringen sker på Säkerhetspolisens eller mottagarens initiativ. Det är också fråga om en överföring när myndigheten gör information tillgänglig för ett tredjeland eller en internationell organisation genom att informationen tillförs ett gemensamt datasystem, t.ex. en databas hos Interpol.

Överföring av personuppgifter till ett tredjeland eller en internationell organisation för behandling där avser bl.a. den situationen att uppgifterna inte behandlas automatiserat i Sverige, utan överförs till ett tredjeland eller en internationell organisation för att automatiseras där. Som exempel kan nämnas blanketter, formulär eller undersökningar som fyllts i för hand och som skickas per post till ett tredjeland där personuppgifterna läggs in i en databas.

Överföring till ett tredjeland eller en internationell organisation får endast göras om de i punkt 1 angivna villkoren och något av alternativen i punkt 2 samtidigt är uppfyllda.

Punkt 1 begränsar till vilka utländska adressater personuppgifter får överföras. Personuppgifter får som huvudregel bara överföras till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland eller till en internationell organisation med brottsbekämpande uppdrag. Möjligheten att i vissa fall överföra personuppgifter till andra regleras i 5 §.

Av kravet på att överföringen ska göras till en brottsbekämpande myndighet följer att den myndighet eller organisation som ska ta emot personuppgifterna ska ha som uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott. Den som personuppgiften överförs till behöver inte ha samma uppgifter som Säkerhetspolisen, men ska ha ett brottsbekämpande uppdrag. När det gäller internationella organisationer är det framför allt Interpol som är av intresse. Även vissa utredningsorgan under FN torde kunna ha brottsbekämpande uppdrag, liksom internationella tribunaler.

I *punkt 2* ställs dessutom krav på viss skyddsnivå för personuppgifter som överförs till ett tredjeland eller till en internationell organisation. Personuppgifter får alltid överföras till ett tredjeland eller till en internationell organisation för vilket eller vilken kommissionen har beslutat att det finns en adekvat skyddsnivå (2 §). Om det inte finns ett sådant beslut får personuppgifterna ändå överföras om uppgifterna kommer att omfattas av tillräckliga skyddsåtgärder hos den som mottar dem (3 §). Finns det inte något beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder får personuppgifter överföras endast när ett undantag för särskilda situationer gäller (4 §). Överföringsgrunderna är alternativa, men ska prövas i den ordning som anges i paragrafen. I första hand ska det alltså prövas om det finns beslut om adekvat skyddsnivå och i andra hand om det finns tillräckliga skyddsåtgärder. Först därefter finns det anledning att bedöma om någon av undantagssituationerna är för handen.

Om personuppgifter ska överföras till en internationell organisation, t.ex. Interpol, är det organisationen som sådan, och inte de enskilda stater som är medlemmar i organisationen, som ska uppfylla kravet på skyddsnivå. Ska personuppgiften skickas till ett tredjeland, men överföringen görs med hjälp av Interpol, ska däremot skyddsnivån i tredjelandet bedömas.

Beslut om adekvat skyddsnivå

2 §

Paragrafen innehåller den första tillåtna grunden för att överföra personuppgifter till ett tredjeland eller till en internationell organisation. Det är först om förutsättningarna i denna paragraf inte är uppfyllda som alternativen att överföra personuppgifter med stöd av reglerna om tillräckliga skyddsåtgärder i 3 § eller särskilda situationer i 4 § ska prövas. Övervägandena finns i avsnitt 17.4.1.

Enligt paragrafen får personuppgifter alltid överföras till ett tredjeland eller en internationell organisation som enligt ett beslut av kommissionen har en adekvat skyddsnivå för personuppgifter. Om kommissionen har meddelat ett sådant beslut för ett territorium eller en sektor i ett tredjeland får personuppgifter överföras dit. Avgränsningen avgörs av innehållet i kommissionens beslut. Eftersom Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av unionsrätten gäller kommissionens beslut inte för myndigheten, men paragrafen ger Säkerhetspolisen samma möjlighet som andra brottsbekämpande myndigheter att överföra personuppgifter till ett tredjeland eller en internationell organisation om det finns ett sådant beslut.

Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation enligt 1 § ska alltid vara uppfyllda för att personuppgifter ska få överföras med stöd av ett beslut om adekvat skyddsnivå.

Om kommissionen beslutar att ett tredjeland, eller en del av det, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå får personuppgifter inte överföras dit med stöd av den nu aktuella paragrafen. Det hindrar dock inte att personuppgifter överförs till tredjelandet eller den internationella organisationen om någon av de andra tillåtna grunderna för överföring är tillämplig.

Tillräckliga skyddsåtgärder

3 §

I paragrafen behandlas den andra tillåtna grunden för överföring av personuppgifter till ett tredjeland eller en internationell organisation. Paragrafen behandlas i avsnitt 17.4.2.

Om det inte finns något beslut om adekvat skyddsnivå enligt 2 § får Säkerhetspolisen ändå överföra personuppgifter till ett tredjeland eller till en internationell organisation, om det finns tillräckliga skyddsåtgärder för uppgifterna där. Förutsättningarna för överföring av personuppgifter enligt 1 § ska alltid vara uppfyllda för att personuppgifter ska få överföras på denna grund.

Enligt *punkt 1* kan tillräckliga skyddsåtgärder finnas om sådana har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade. Personuppgifter kan normalt överföras till länder som är anslutna till dataskyddskonventionen eller har ingått bindande avtal om internationellt samarbete som innehåller dataskyddsregler som är tillämpliga på överföringen. Det kan också vara fråga om bilaterala avtal som Sverige ingått med ett tredjeland och som sörjer för att kravet på dataskydd uppfylls och registrerades rättigheter respekteras.

Enligt *punkt 2* får personuppgifter också överföras om den myndighet eller organisation som ska ta emot uppgifterna, på annat sätt än genom avtal, garanterar tillräckligt skydd för dem. Säkerhetspolisen ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Exempel på sådant som kan vägas in vid bedömningen av om tillräckligt skydd garanteras är bl.a. bindande åtaganden att inte sprida personuppgifterna vidare eller att inte använda personuppgifterna efter viss tidpunkt.

Överföring i särskilda situationer

4 §

Paragrafen reglerar möjligheten att överföra personuppgifter till ett tredjeland eller till en internationell organisation när det varken finns beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder för uppgifterna. Kravet är då att det ska vara fråga om en särskild situation. Övervägandena finns i avsnitt 17.4.3.

Undantagen för särskilda situationer gäller även samlingar av överföringar. Med samling avses här flera överföringar som på något sätt är sammankopplade, antingen därför att det är flera personuppgifter som överförs inom ramen för ett ärende, eller för att det är en personuppgift som överförs till flera adressater. En överföring kan också innehålla flera personuppgifter och därmed utgöra en samling, t.ex. ett utdrag från ett register. Det viktiga när det gäller samlingar av överföringar är att det i efterhand går att kontrollera vilka personuppgifter som har överförts.

Överföringen ska enligt *första stycket* vara nödvändig i någon av de särskilda situationer som räknas upp i punkterna 1–4. Punkterna är alternativa. I punkterna 2 och 3 föreskrivs att överföringen ska vara nödvändig i det enskilda fallet. Oavsett vilken situation som är för handen ska förutsättningarna för överföring till tredjeland och internationella organisationer i 1 § alltid vara uppfyllda.

I *punkt 1* regleras två situationer som kan göra överföringen nödvändig. Det är dels för att värna vitala intressen för den registrerade eller någon annan fysisk person, dels för att värna andra berättigade intressen som den registrerade har. I det sistnämnda fallet gäller alltså inte skyddet till förmån för någon annan än den vars personuppgifter ska överföras. Den som är misstänkt för ett brott kan ha ett berättigat intresse av att viss bevisning som finns i ett tredjeland inhämtas därifrån. Ett vittne som befinner sig i ett tredjeland kan ha ett berättigat intresse av att hans eller hennes personuppgifter överförs dit för att ett förhör ska kunna komma till stånd där.

När det gäller skyddet för vitala intressen kan det gälla både för den som personuppgiften avser och för någon annan fysisk person. Det kan t.ex. handla om att överföra uppgifter om en person som misstänks planera ett sprängdåd. Även andra för den enskilde väsentliga intressen som inte är direkt avgörande för liv och död, t.ex. hälsa och ekonomiska intressen, kan värnas med stöd av undantaget för vitala intressen.

Punkt 2 tillgodoser behovet av att i ett enskilt fall kunna överföra personuppgifter till ett tredjeland eller en internationell organisation för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Som exempel kan nämnas att Säkerhetspolisen i ett

enskilt fall har information om att en misstänkt terrorist befinner sig i landet, men personen identifieras först när han eller hon har rest till ett tredjeland och kan antas komma att begå brott där. Åtgärden behöver inte vara nödvändig för att tillgodose Säkerhetspolisens behov och intressen. Det kan finnas förutsättningar för att tillämpa punkten om ett tredjeland behöver få tillgång till svenska personuppgifter, t.ex. uppgift om att en person är dömd för ett visst brott. Personuppgifter kan lämnas både på begäran och på Säkerhetspolisens eget initiativ.

Punkt 3 innebär att personuppgifter kan överföras till ett tredjeland eller en internationell organisation om överföringen är nödvändig i ett enskilt fall för att kunna fastställa, göra gällande eller försvara ett rättsligt anspråk. Det rättsliga anspråket ska vara hänförligt till ett ändamål som omfattas av lagens tillämpningsområde. Exempel på sådana rättsliga anspråk är bl.a. skadestånd i anledning av brott.

Ett exempel på när det kan vara nödvändigt att överföra personuppgifter enligt *punkt 4* för att avvärja en omedelbar och allvarlig fara för allmän säkerhet är om det finns information om ett förestående terroristattentat. Det kan vara fråga om allmän säkerhet i Sverige eller i någon annan stat. Om det är fråga om en omedelbar fara för allmän säkerhet utomlands ligger det i sakens natur att Säkerhetspolisen har fått veta något av intresse som det är viktigt att tredjelandet eller den internationella organisationen får information om direkt, t.ex. planer på en flygplanskapning. Säkerhetspolisen kan naturligtvis bara beakta sådant som den känner till vid prövningen av om personuppgifterna får överföras. Att det sedan i efterhand visar sig att överföringen inte var nödvändig, t.ex. därför att faran aldrig realiserades, innebär inte att överföringen var otillåten.

Enligt *andra stycket* ska en intresseavvägning göras när personuppgifter ska överföras enligt punkt 2 eller 3. De intressen som ska vägas mot varandra är skyddet för den registrerades rättigheter och friheter och det allmännas intresse av att överföringen görs. Om den registrerades intresse väger tyngre än det allmännas får personuppgifterna inte överföras. Ett exempel där den registrerades intresse väger tyngre kan vara om han eller hon riskerar dödsstraff, kroppsstraff eller tortyr om hans eller hennes personuppgifter överförs till ett tredjeland.

Överföring till andra mottagare

5 §

Paragrafen är ett undantag från kravet i 1 § första stycket 1 att överföring av personuppgifter till tredjeland ska göras till brottsbekämpande myndigheter eller underrättelse- och säkerhetstjänster i tredjeland. Om förutsättningarna i paragrafen är uppfyllda får personuppgifter överföras även till andra än sådana. Det kan t.ex. vara företag och privatpersoner i ett tredjeland. Det kan också vara fråga om överföring till andra kategorier av myndigheter än de som anges i 1 § första stycket, t.ex. en specialmyndighet som hanterar frågor om finansiering av terrorism. Överföring till andra mottagare får dock endast göras om samtliga i första stycket angivna förutsättningar är uppfyllda. Dessutom ska de övriga förutsättningarna i 1 § vara uppfyllda. Övervägandena finns i avsnitt 17.5.

Enligt *första stycket punkt 1* ska överföringen vara absolut nödvändig för att Säkerhetspolisen ska kunna utföra en uppgift som anges i 2 kap.

1 §. Kravet på absolut nödvändighet innebär att överföringen inte kan underlåtas. Ett exempel kan vara att Säkerhetspolisen i sin underrättelseverksamhet behöver kontakta ett privat företag i ett tredjeland för att få fram information som behövs omedelbart i den brottsbekämpande verksamheten.

Enligt *punkt 2* krävs också att Säkerhetspolisen bedömer att det skulle vara ineffektivt eller på något annat sätt olämpligt att i stället överföra personuppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet. Det kan vara något i tidigare kontakter med myndigheten i det landet eller andra indikationer som ger anledning att tro att syftet med överföringen kan komma att förfelas eller att det på något annat sätt skulle vara olämpligt att överföra personuppgifterna via den myndigheten. Ett exempel är överföringar till olika internetoperatörer i syfte att t.ex. identifiera och kartlägga misstänkta terrorister och andra personer som kan utgöra säkerhetshot. Det skulle vara ineffektivt om varje sådan överföring skulle behöva göras genom en myndighet i mottagarlandet med hänsyn både till mängden förfrågningar och till den brådska som ofta råder. Ett annat exempel är information som lämnas till en bank för att förhindra att banken utnyttjas för brottsliga penningöverföringar, t.ex. finansiering av terrorism. I sådana fall kan kontakt behöva tas omedelbart.

Enligt *andra stycket* ska det göras en intresseavvägning mellan den registrerades intresse av skydd mot kränkning av rättigheter och friheter och det allmännas intresse av att överföringen kommer till stånd. Om den enskildes skyddsintresse väger tyngre får överföringen inte göras. Ett exempel kan vara om personen som uppgifterna avser riskerar förföljelse på grund av sin religion eller politiska åskådning om personuppgifterna överförs till någon annan än de som anges i 1 § 1. Intresseavvägningen motsvarar den som enligt 4 § andra stycket ska göras när personuppgifter ska överföras i vissa särskilda situationer.

Ikraftträdande- och övergångsbestämmelser

Ikraftträdande och övergångsbestämmelserna behandlas i avsnitt 19.

Punkt 1 föreskriver när lagen ska träda i kraft.

I *punkt 2* föreskrivs att bestämmelsen om loggning i 5 kap. 4 § tillämpas från och med den 1 oktober 2024 på sådana automatiserade behandlingssystem som inrättats före den 1 januari 2020.

I *punkt 3* föreskrivs att äldre föreskrifter fortfarande ska gälla för överklagande av beslut om behandling av personuppgifter inom denna lags tillämpningsområde som har meddelats före ikraftträdandet. Med äldre föreskrifter avses här personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191). Punkten tar inte bara sikte på själva överklagandet utan också på vilket regelverk som ska tillämpas när överklagandet prövas. Äldre föreskrifter i polisdatalagen (2010:361) och föreskrifter som har meddelats i anslutning till den ska då tillämpas.

21.2 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

I paragrafen anges vad Säkerhets- och integritetsskyddsnämnden utövar tillsyn över. Övervägandena finns i avsnitt 15.7.

Första stycket är oförändrat.

I *andra stycket* läggs till att nämndens tillsyn även omfattar sådan behandling av personuppgifter som utförs av Säkerhetspolisen och Polismyndigheten enligt lagen om Säkerhetspolisens behandling av personuppgifter. Där förtydligas också att tillsynen särskilt ska avse behandling av känsliga personuppgifter.

Tredje och fjärde styckena är oförändrade.

Ikraftträdande och övergångsbestämmelserna

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 19.

Punkt 1 föreskriver när lagen ska träda i kraft.

Punkt 2 innebär att Säkerhets- och integritetsskyddsnämndens tillsyn över Säkerhetspolisens, Polismyndighetens och Ekobrottsmyndighetens personuppgiftsbehandling fortfarande regleras enligt de äldre regelverken avseende förhållanden före ikraftträdandet den 1 januari 2020. Det innebär att nämndens tillsyn således även omfattar Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (2010:362) och polisdatalagen (1998:622) respektive Polismyndighetens och Ekobrottsmyndighetens behandling av personuppgifter enligt polisdatalagen (2010:362).

21.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

2 §

Paragrafen reglerar sekretess till skydd för underrättelseverksamhet. Övervägandena finns i avsnitt 18.

I *andra stycket* läggs en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter till. Ändringen innebär ingen ändring i sak av den ordning som gäller i dag.

Första, tredje och *fjärde styckena* är oförändrade.

35 kap

1 §

Paragrafen reglerar sekretess för enskilds personliga och ekonomiska förhållanden i viss brottsbekämpande verksamhet. Övervägandena finns i avsnitt 18.

I *första stycket femte punkten* läggs det till en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter. Bestämmelsen, som för Säkerhetspolisens del tidigare hänvisade till 6 kap. polisdatalagen (2010:361), ändrades i samband med att lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område infördes (prop. 2017/18:269 s. 277 f.). Genom en övergångsbestämmelse till den lagen har 6 kap. polisdatalagen fortsatt att gälla för Säkerhetspolisens del. Övergångsbestämmelsen upphör dock att gälla vid införandet av den nya lagen om Säkerhetspolisens behandling av personuppgifter Ändringen i nu aktuell paragraf innebär ingen ändring i sak av vad som gäller i dag.

Andra–fjärde styckena är oförändrade.

10 §

Paragrafen innehåller hänvisningar till sekretessbrytande bestämmelser i ett antal andra lagar. Övervägandena finns i avsnitt 18. I paragrafen läggs det till en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter till. Ändringen innebär ingen ändring i sak av vad som gäller i dag.

21.4 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

6 kap.

1 §

I paragrafen regleras hur bestämmelserna i lagen förhåller sig till andra bestämmelser om behandling av personuppgifter. Övervägandena finns i avsnitt 18.

I paragrafen läggs det till en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter till. Det innebär att den lagen gäller vid behandling av personuppgifter i internationellt polisiärt samarbete, om det inte finns avvikande bestämmelser i lagen om internationellt polisiärt samarbete eller föreskrifter som regeringen har meddelat i anslutning till den.

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

1 kap.

3 §

Paragrafen reglerar undantag från bestämmelsen i 2 §, som utsträcker dataskyddsförordningens tillämpningsområde. I paragrafen ersätts hänvisningen till 6 kap. polisdatalagen (2010:361) med en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter. Övervägandena finns i avsnitt 18.

21.6 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

3 kap.

13 §

I paragrafen anges vad som avses med registerkontroll. En hänvisning till lagen om Säkerhetspolisens personuppgiftsbehandling läggs till. Ändringen innebär inte någon ändring i sak av den ordning som gäller i dag. Övervägandena finns i avsnitt 18.

14 §

I paragrafen anges när registerkontroll ska göras. I *andra* och *tredje styckena* läggs en hänvisning till lagen om Säkerhetspolisens behandling av personuppgifter till, vilket inte innebär någon ändring i sak av den ordning som gäller i dag. *Första* och *fjärde styckena* är oförändrade. Övervägandena finns i avsnitt 18.

21.7 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Genom ändringen upphör punkt 4 i ikraftträdande- och övergångsbestämmelserna till lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område att gälla. Övervägandena finns i avsnitt 18.

När lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område infördes upphävdes polisdatalagen (2010:361). Genom en övergångsbestämmelse fortsatte polisdatalagen att gälla för Säkerhetspolisens personuppgiftsbehandling på området för nationell säkerhet. När Säkerhetspolisens nya datalag införs behövs inte längre övergångsbestämmelsen.

Sammanfattning av betänkandet Brottsdatalag – kompletterande lagstiftning (SOU 2017:74)

En ny lag för Säkerhetspolisen

Regleringen utgår från dagens reglering och brottsdatalagen

Utredningen föreslår att det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter, Säkerhetspolisens datalag, som ersätter regleringen i polisdatalagen. Den regleringen ska bilda mönster för den nya lagen, som ska vara heltäckande och därför blir betydligt mer omfattande än dagens reglering. Den nya lagen följer i princip brottsdatalagens systematik och innehåll. Det innebär att bestämmelserna om grundläggande krav på behandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, rättsmedel och överföring av personuppgifter till tredjeland i stort sett överensstämmer med brottsdatalagens bestämmelser.

Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. När Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra brott ska myndigheten tillämpa brottsdatalagen och polisens brottsdatalag.

Rättslig grund för behandling av personuppgifter

Regleringen av för vilka ändamål Säkerhetspolisen får behandla personuppgifter är i dag uppdelad i primära och sekundära ändamål. Regleringen behålls i stort sett oförändrad men det tydliggörs att det är fråga om bestämmelser om rättslig grund – rättslig grund för behandling och rättslig grund för utlämnande.

Behandling av känsliga personuppgifter

Huvudregeln är att Säkerhetspolisen på samma sätt som i dag inte ska få behandla känsliga personuppgifter. Om uppgifter om en person redan behandlas ska de dock få kompletteras med känsliga personuppgifter om det är absolut nödvändigt.

Säkerhetspolisen får i dag använda uppgifter som avslöjar känsliga personuppgifter som sökbegrepp om det är absolut nödvändigt. Utredningen föreslår att samma sökförbud som i brottsdatalagen ska gälla för Säkerhetspolisen, dvs. att det ska vara förbjudet att göra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Från förbudet görs det undantag. Det ska vara tillåtet att använda brottsrubriceringar, uppgifter om tillvägagångssätt vid brott och uppgifter som beskriver en persons utseende vid sökning. Även sökningar i syfte att få fram personurval grundat på flertalet känsliga personuppgifter ska tillåtas, om sökningen är absolut nödvändig.

Elektroniskt utlämnande

Säkerhetspolisen ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Säkerhetspolisen ska få medge Polismyndigheten, Försvarsmakten och Försvarets radioanstalt direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften. Även underrättelse- och säkerhetstjänster inom EU och EES ska få medges direktåtkomst till uppgifter som Säkerhetspolisen behandlar för vissa syften om det behövs för samarbetet mot terrorism. Sådan direktåtkomst ska dock endast få medges till personuppgifter i en avskild uppgiftssamling och regeringen ska underrättas innan direktåtkomst medges.

Längsta tid för behandling

Personuppgifter ska inte få behandlas under längre tid än vad som behövs för något eller några av de syften för vilka Säkerhetspolisen får behandla personuppgifter. Huvudregeln ska på samma sätt som i dag vara att personuppgifter som har gjorts gemensamt tillgängliga inte får behandlas längre än tio år efter det år då den senaste registreringen avseende personen gjordes. Uppgifter om personer som ännu inte fyllt 18 år ska dock inte få behandlas längre än fem år från den senaste registreringen. Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken ska inte få behandlas längre än 40 år efter det år då den senaste registreringen gjordes. På samma sätt som i dag ska Säkerhetspolisen kunna besluta att personuppgifter får behandlas under längre tid om det finns särskilda skäl.

Tillsyn över Säkerhetspolisens personuppgiftsbehandling

Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden ska på i huvudsak samma sätt som i dag utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling.

Datainspektionen ska utöva allmän tillsyn över personuppgifts-behandling enligt den nya lagen och ge råd och stöd till Säkerhetspolisen. Inspektionen ska i huvudsak ha samma befogenheter som enligt brottsdatalagen. Säkerhetspolisen ska dock inte kunna påföras administrativ sanktionsavgift.

Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling och på begäran av enskild kontrollera om behandlingen av personuppgifter är författningsenlig.

Ikraftträdande och övergångsbestämmelser

De nya lagen och övriga författningsändringar föreslås träda i kraft den 1 maj 2018. Till den nya lagen krävs det övergångsbestämmelser för ärenden om tillsyn som har påbörjats före ikraftträdandet men inte hunnit slutföras och för mål som har överklagats men som inte har hunnit slutföras inom den tiden. Det krävs också en särskild övergångsbestämmelse för ersättning av skador som har vållats före ikraftträdandet.

Betänkandets lagförslag

Förslag till Säkerhetspolisens datalag (2018:000)

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

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

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Lagen gäller i tillämpliga delar vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning.

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

Förhållandet till annan reglering

4 § I lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns det särskilda bestämmelser om behandling av personuppgifter som följer av internationella överenskommelser. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

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

6 § I brottsdatalagen (2018:000) och polisens brottsdatalag (2010:361) finns det bestämmelser om Säkerhetspolisens behandling av personuppgifter i frågor som inte rör nationell säkerhet.

Personuppgiftsansvar

7 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

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

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

Uttryck i lagen

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

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.
Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av

	en överenskommelse mellan två eller flera stater.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften rör.
Tillsynsmyndighet	Den myndighet som regeringen utser att enligt denna lag utöva tillsyn över personuppgifts–behandling.
Tredjeland	En stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgift som rör hälsa	Personuppgift som rör en persons fysiska eller psykiska hälsa, inkluderande information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

Lagens tillämpning på uppgifter om juridiska personer

10 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 7 § om personuppgiftsansvar,
2. 2 kap. 1–3 §§ om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 och 3 §§ om gemensamt tillgängliga uppgifter,
4. 4 kap. 1–4 och 6–11 §§ om längsta tid som personuppgifter får behandlas, och
5. 5 kap. 5 § om tillgången till personuppgifter.

2 kap. Behandling av personuppgifter

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
   a) brott mot rikets säkerhet,
   b) terrorbrott, eller
   c) tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,
2. utreda eller lagföra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra uppgifter
   a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
   b) enligt säkerhetsskyddslagen (1996:627), eller
   c) enligt utlännings- och medborgarskapslagstiftningen,
4. fullgöra annan arbetsuppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen, eller
5. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

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

1. för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,
3. i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelse–verksamhet, om det finns särskilda skäl att tillhandahålla informationen,
4. i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med viss uppgift,
5. i brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller

6. i verksamhet hos utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter som behandlas med stöd av 1 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra.

I ett enskilt fall får personuppgifter som behandlas med stöd av 1 § även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första och andra styckena, under förutsättning att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

3 § Personuppgifter får även behandlas om
1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för handläggningen.

Ändamål för behandling av personuppgifter

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

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

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

Grundläggande krav på behandling av personuppgifter

Laglig och korrekt behandling

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

Personuppgifternas kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

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

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Känsliga personuppgifter

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

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

10 § Säkerhetspolisen får behandla biometriska uppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen. Genetiska uppgifter får inte behandlas.

11 § Personuppgifter som avses i 9 och 10 §§ betecknas som känsliga personuppgifter. Känsliga personuppgifter får behandlas med stöd av 3 §.

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

Första stycket hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

Första stycket hindrar inte heller sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för något av de syften som anges i 1 §.

Åtgärder för att säkerställa personuppgifternas kvalitet

13 § Alla rimliga åtgärder ska vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

14 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–11 § utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska Säkerhetspolisen i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Uppgiftsskyldighet och utlämnande av personuppgifter

15 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

16 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott, eller
2. utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

17 § Polismyndigheten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som behandlas med stöd av 1 § första stycket 1–3 a, om myndigheten behöver uppgifterna för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2 polisens brottsdatalag (2010:361).

18 § Försvarets radioanstalt och Försvarsmakten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som be-handlas med stöd av 1 § första stycket 1 eller 2, om den mottagande myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst.

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

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 5–7 §§.

Personuppgifter från transportföretag

20 § Personuppgifter som tillhandahålls Säkerhetspolisen enligt 25 § polislagen (1984:387) får behandlas för något av de syften som anges i 1 § första stycket 1–3 a.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål.

21 § Vid terminalåtkomst enligt 26 § polislagen (1984:387) får Säkerhetspolisen inte ändra eller på annat sätt bearbeta personuppgifterna.

Föreskrifter

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

1. att personuppgifter får lämnas ut i andra fall än som anges i 15–18 §§,
2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 19 § första stycket,
3. underrättelseskyldighet, och
4. sökning i personuppgifter.

3 kap. Gemensamt tillgängliga uppgifter

Allmän bestämmelse

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Personuppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 3 §.

Personuppgifter som får göras gemensamt tillgängliga

2 § Personuppgifter får göras gemensamt tillgängliga om det behövs för något av de syften som anges i 2 kap. 1 §.

Särskilda upplysningar

3 § Om det inte framgår av sammanhanget eller på något annat sätt för vilket ändamål som gemensamt tillgängliga personuppgifter behandlas, ska det tydliggöras genom en särskild upplysning.

4 § Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt för brott eller brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 eller 2.

Uppgifter om en person som kan antas ha direkt samband med sådan brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon upplysning behöver dock inte lämnas om det på grund av omständigheterna är onödigt.

Någon upplysning enligt andra stycket behöver inte heller lämnas om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till och
2. bearbetningen av uppgifterna inte har genomförts.

Direktåtkomst

5 § Polismyndigheten får för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2 polisens brottsdatalag (2010:361) medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1–3 a. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

6 § Försvarets radioanstalt och Försvarsmakten får i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 eller 2. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

7 § Om det behövs för samarbetet mot terrorism får en underrättelse eller säkerhetstjänst i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet medges direktåtkomst till personuppgifter i en avskild uppgiftssamling som Säkerhetspolisen upprättat i syfte att dela information med sådana mottagare. Uppgiftssamlingen får endast innehålla personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 b och har gjorts gemensamt tillgängliga.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt första stycket ska Säkerhetspolisen underrätta regeringen.

Föreskrifter

8 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om underrättelseskyldighet vid direktåtkomst.

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomst enligt 5–7 §§ och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Personuppgifter får inte behandlas under längre tid än vad som behövs för något eller några av de syften som anges i 2 kap. 1–3 §§.

Det som sägs i första stycket hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Vid automatiserad behandling gäller också de begränsningar som följer av 2–11 §§.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 § Trots det som sägs i 1 § andra stycket får personuppgifter som inte har gjorts gemensamt tillgängliga inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller
2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Första stycket gäller inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

4 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts ner eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter

utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångs–balken.

5 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga gemensamt tillgängliga uppgifter

6 § Trots det som sägs i 1 § andra stycket får andra personuppgifter än de som anges i 3 och 4 §§ och som har gjorts gemensamt tillgängliga som längst behandlas under den tid som anges i 7–11 §§.

7 § Personuppgifter som behandlas för något av de syften som anges i 2 kap. 1 § första stycket 1 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unges anknytning till brottslig verksamhet, om någon ny registrering inte gjorts efter det att han eller hon fyllt 18 år.

8 § Personuppgifter som behandlas för något av de syften som anges i 2 kap. 1 § första stycket 3–5 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge, om någon ny registrering inte gjorts efter det att han eller hon fyllt 18 år.

9 § Personuppgifter som behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket får inte behandlas längre än

1. tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet, om uppgifterna behandlas för något av de syften som anges i 2 kap. 1 § första stycket 1, och
2. tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen, om uppgifterna behandlas för något av de syften som anges i 2 kap. 1 § första stycket 3–5.

10 § Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken som utövas av främmande makt, får inte behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. För personuppgifter som

behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket gäller 9 §.

11 § Om det finns särskilda skäl får Säkerhetspolisen besluta att personuppgifter får behandlas under längre tid än vad som anges i 7–10 §§, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Om personuppgifter behandlas med stöd av ett sådant beslut ska frågan om fortsatt behandling prövas på nytt senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i 9 §, senast vid utgången av det tredje kalenderåret efter beslutet. Tiden som personuppgifterna får behandlas får vid varje tillfälle förlängas med längst tio år eller, om det är fråga om uppgifter som avses i 9 §, med längst tre år.

Föreskrifter

12 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3 och 4 §§.

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

1. att personuppgifter, med avvikelse från 2 § första stycket och 7–11 §§, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Skyldigheter som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

1 § Säkerhetspolisen ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

2 § Både vid beslut om hur behandlingen ska utföras och vid behandlingen ska Säkerhetspolisen, genom lämpliga tekniska och organisatoriska åtgärder, se till att dataskyddsprinciper säkerställs på ett effektivt sätt och att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

3 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem som regel endast är möjligt att behandla de personuppgifter som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

4 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

5 § Säkerhetspolisen ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

6 § Kan en typ av ny behandling, eller betydande förändringar avseende redan pågående behandling, antas medföra särskild risk för intrång i registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Säkerheten för personuppgifter

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

Samarbete med tillsynsmyndigheten

8 § Säkerhetspolisen ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till den.

Dataskyddsombud

9 § Säkerhetspolisen ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när data-skyddsombud utses och entledigas.

10 § Dataskyddsombud ska

1. självständigt kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge Säkerhetspolisen råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och

5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

11 § Om Säkerhetspolisen bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Personuppgiftsbiträden

12 § Säkerhetspolisen får, om det är lämpligt, anlita personupp–giftsbiträden. När ett personuppgiftsbiträde anlitas, ska Säkerhetspolisen försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

13 § Det ska finnas ett skriftligt avtal eller annan skriftlig överens–kommelse om personuppgiftsbiträdets behandling av personuppgifter för Säkerhetspolisens räkning.

Ett personuppgiftsbiträde får inte utan skriftligt tillstånd av Säkerhetspolisen anlita ett annat personuppgiftsbiträde.

14 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från Säkerhetspolisen.

Om ett personuppgiftsbiträde i strid med Säkerhetspolisens instruktioner fastställer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den be-handlingen.

15 § Det som sägs om Säkerhetspolisens skyldigheter i 4, 5, 7 och 8 §§ gäller även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

Föreskrifter

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

1. åtgärder som avses i 1–4, 6 och 7 §§,
2. tillgången till personuppgifter,
3. skyldigheten att föra register över kategorier av behandling av personuppgifter,
4. skyldigheten att införa interna rutiner för anmälan av överträdelser, och
5. innehållet i avtal och överenskommelser enligt 13 §.

6 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Säkerhetspolisen ska göra följande allmänna information tillgänglig för registrerade.

1. Myndighetens identitet och kontaktuppgifter.
2. Dataskyddsombudets kontaktuppgifter.
3. Ändamålen med behandlingen.
4. Rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 och 7 §§.

Personrelaterad information

2 § Säkerhetspolisen ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

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

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

Begränsning av rätten till information

3 § Informationsskyldigheten i 2 § gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Om förutsättningarna i första stycket är uppfyllda, är Säkerhetspolisen inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 eller 7 §.

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

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

5 § Om en begäran enligt 2 § är orimlig eller uppenbart ogrundad får Säkerhetspolisen avslå den.

Av 9 § andra stycket framgår att Säkerhetspolisen i vissa fall får ta ut avgift i stället för att avslå begäran.

Rätten till rättelse, radering och begränsning av behandlingen

6 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om Säkerhetspolisen inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

7 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne om de behandlas i strid med 2 kap. 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–11 §. Detsamma gäller om radering krävs för att Säkerhetspolisen ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska Säkerhetspolisen på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

8 § Säkerhetspolisen avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

9 § Information enligt 1 § ska lämnas utan avgift. Information och uppgifter enligt 2 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 2 § oftare än en gång per år, får Säkerhetspolisen ta ut en rimlig avgift eller avslå begäran enligt 5 § första stycket.

Föreskrifter

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

1. information enligt 1 och 2 §§,
2. avgift för information som avses i 2 §, och
3. kraven på en begäran enligt 2, 6 eller 7 §.

7 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling, och
2. ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd eller när det i övrigt är påkallat.

2 § Bestämmelser om tillsyn över Säkerhetspolisens behandling av personuppgifter finns även i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Befogenheter

Undersökningsbefogenheter

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

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller ett personuppgiftsbiträde disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

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

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

Korrigerande befogenheter

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

1. genom sådana åtgärder som anges i 4 § första stycket försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter, eller
3. förbjuda fortsatt behandling om bristen är allvarlig.

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

Kommunikation

6 § Innan tillsynsmyndigheten fattar ett beslut enligt 5 § första stycket 2 eller 3, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

8 kap. Skadestånd och rättsmedel

Skadestånd

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

Överklagande

Överklagande av Säkerhetspolisens beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 6 kap. 6 § första stycket, radering enligt 6 kap. 7 § första stycket eller begränsning av behandlingen enligt 6 kap. 6 § andra stycket eller 6 kap. 7 § andra stycket, som har meddelats av Säkerhetspolisen i egenskap av person–uppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 6 kap. 2 § eller att ta ut avgift enligt 6 kap. 9 § andra stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till den får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som inte får överklagas

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

9 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Grundläggande förutsättningar för överföring

1 § Säkerhetspolisen får överföra personuppgifter som behandlas till ett tredjeland eller en internationell organisation. Det gäller även överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. riktas till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland eller en internationell organisation med brottsbekämpande uppdrag och
2. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 3 §, eller
b) tillräckliga skyddsåtgärder enligt 4 §, eller
c) ett undantag för särskilda situationer enligt 5 §.

2 § Personuppgifter som Säkerhetspolisen har fått från en annan stat får överföras till ett tredjeland eller en internationell organisation endast om

den stat som lämnat uppgifterna till Säkerhetspolisen har medgett att de överförs.

Tillåtna grunder för överföring

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

4 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter, eller
2. den myndighet eller organisation som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får personuppgifter överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. skydda den registrerades eller en annan fysisk persons vitala intressen, eller andra berättigade intressen för den registrerade,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Överföring till andra mottagare

6 § Säkerhetspolisen får i ett enskilt fall överföra personuppgifter till någon annan mottagare än som anges i 1 § i ett tredjeland. Personuppgifterna får överföras endast om

1. det är absolut nödvändigt för att Säkerhetspolisen ska kunna utföra en arbetsuppgift enligt 2 kap. 1 eller 2 § och
2. det skulle vara ineffektivt eller olämpligt att överföra dem till en mottagare som anges i 1 § i det tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Villkor om användningsbegränsning

7 § Om Säkerhetspolisen har fått personuppgifter från ett tredjeland eller en internationell organisation och det på grund av en överenskommelse med det tredjelandet eller den internationella organisationen gäller villkor som begränsar möjligheten att använda uppgifterna, ska Säkerhetspolisen följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

8 § Säkerhetspolisen får, vid överföring av personuppgifter till ett tredjeland eller en internationell organisation, ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs från allmän synpunkt eller med hänsyn till enskilds rätt.

Föreskrifter

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om dokumentation av överföringar.

---

1. Denna lag träder i kraft den 1 maj 2018.

2. Bestämmelsen i 5 kap. 4 § om loggning behöver inte tillämpas på automatiserade behandlingssystem som inrättats före ikraftträdandet förrän den 1 maj 2023.

3. Ärenden om tillsyn över Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet i myndighetens brottsbekämpande eller lagförande verksamhet och som Datainspektionen eller Säkerhets- och integritetsskyddsnämnden inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.

4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som meddelats före ikraftträdandet och som rör behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

5. Bestämmelsen om skadestånd i 48 § i personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12 § säkerhetsskyddslagen (1996:627) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
12 §[1]	
Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstanke–register *eller lagen (2010:362) om polisens allmänna spanings–register*. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av *polisdatalagen* (2010:361).	Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister *eller* lagen (1998:621) om misstanke–register. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av *polisens brottsdatalag* (2010:361) *eller Säkerhetspolisens data–lag (2018:000)*.

Denna lag träder i kraft den 1 maj 2018

[1] Senaste lydelse 2010:365.

Bilaga 2

Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1, 3 och 4 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt SOU 2016:65	*Föreslagen lydelse*
1 §	
Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över *behandlingen* av personuppgifter i *Säkerhetspolisens* brottsbekämpande verksamhet. Tillsynen ska särskilt avse sådan behandling som avses i *2 kap. 10 § polisdatalagen (2010:361).*	Nämnden ska även utöva tillsyn över *Säkerhetspolisens behandling* av personuppgifter *som rör nationell säkerhet* i brottsbekämpande *och lagförande* verksamhet. Tillsynen ska särskilt avse sådan behandling som avses i *2 kap. 9 och 10 §§ Säkerhetspolisens datalag (2018:000).*
	Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.
Nuvarande lydelse	*Föreslagen lydelse*
3 §	
Nämnden är skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för sådana tvångsmedel *eller varit föremål för sådan personuppgiftsbehandling* som avses i 1 § och om användningen av *tvångsmedel* och därmed sammanhängande verksamhet *eller behandlingen av personuppgifter* har *skett* i enlighet med lag eller annan författning. *Nämnden skall underrätta den enskilde om att kontrollen har utförts.*	Nämnden är skyldig att på begäran av en enskild kontrollera om han eller hon
	1. har utsatts för sådana tvångsmedel som avses i 1 § och om användningen av *dem* och därmed sammanhängande verksamhet har *varit* i enlighet med lag eller annan författning, *eller*
	2. varit föremål för sådan personuppgiftsbehandling som avses i 1 § och om den har utförts i enlighet med lag eller annan författning.
	Nämnden ska underrätta den enskilde om att kontrollen har utförts.

	Nämnden får vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad.
4 §	
Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Även domstolar samt de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär.	Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter *och upplysningar, den information* och det biträde som nämnden begär. Även domstolar och de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär.

Denna lag träder ikraft den 1 maj 2018.

Bilaga 2

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 2 §, 35 kap. 1, 4 b och 10 §§ offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
2 §[1]	
Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. *7 § 1* eller *6 kap. 1 § 1 polisdatalagen* (2010:361), om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.	Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. *1 § första stycket 1 polisens brottsdatalag* (2010:361) eller 2 *kap. 1 § första stycket 1 Säkerhetspolisens data–lag (2018:000),* om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.
Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till	Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till *sådan verksamhet som avses i*
1. *sådan verksamhet som avses i 2 kap. 5 § 1 skattebrottsdatalagen (2017:452),*	1. *2 kap. 1 § första stycket 1 Kustbevakningens brottsdatalag (2012:145),*
2. *sådan verksamhet som avses i* 2 kap. *5 § 1 tullbrottsdatalagen* (2017:447), eller	2. 2 kap. *1 § första stycket 1 Tullverkets brottsdatalag* (2017:447), eller
3. *sådan verksamhet som avses i 3 kap. 2 § 1 kustbevakningsdatalagen (2012:145).*	3. *2 kap. 1 § första stycket 1 Skatteverkets brottsdatalag (2017:452).*

Sekretess enligt första stycket gäller inte för uppgift som hänför sig till verksamhet hos Säkerhetspolisen och som har förts in i en allmän handling före år 1949.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Lydelse enligt prop. 2016/17:208	*Föreslagen lydelse*
35 kap.	
1 §	
Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den	

[1] Senaste lydelse 2017:456.

enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,

3. angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt *4* kap. *polisdatalagen* (2010:361) eller som annars behandlas med stöd av de bestämmelserna eller uppgifter som behandlas av Säkerhetspolisen med stöd av *6 kap. samma lag*,	5. register som förs av Polismyndigheten enligt *5* kap. *polisens brottsdatalag* (2010:361) eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen med stöd av *Säkerhetspolisens datalag (2018:000)*,
6. register som förs enligt lagen (1998:621) om misstankeregister,	
7. register som förs av Skatteverket enligt *skattebrottsdatalagen* (2017:452) eller som annars behandlas där med stöd av samma lag,	7. register som förs av Skatteverket enligt *Skatteverkets brottsdatalag* (2017:452) eller som annars behandlas där med stöd av samma lag,
8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,	8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, *eller*
9. register som förs av Tullverket enligt *tullbrottsdatalagen* (2017:447) eller som annars behandlas där med stöd av samma lag, *eller*	9. register som förs av Tullverket enligt *Tullverkets brottsdatalag* (2017:447) eller som annars behandlas där med stöd av samma lag.
10. register som förs enligt lagen (2010:362) om polisens allmänna spaningsregister.	

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Lydelse enligt SOU 2017:29	*Föreslagen lydelse*
4 b §	
Sekretess gäller hos en behörig myndighet enligt brottsdatalagen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag.	Sekretess gäller hos *1.* en behörig myndighet enligt brottsdatalagen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag, och *2. Säkerhetspolisen för uppgift i ett sådant personurval som avses i 2 kap. 12 § Säkerhetspolisens datalag (2018:000).*
För uppgift i en allmän handling gäller sekretessen högst sjuttio år.	För uppgift i en allmän handling gäller sekretessen *i* högst sjuttio år.

Nuvarande lydelse	*Föreslagen lydelse*
10 §[2]	
Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut	
1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,	
2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) *samt* i förordning som har meddelats med stöd i den lagen,	2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) *och* i förordning som har meddelats med stöd i den lagen,
	3. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken,
3. enligt vad som föreskrivs i – lagen (1998:621) om misstankeregister,	*4.* enligt vad som föreskrivs i
– *polisdatalagen* (2010:361),	– *polisens brottsdatalag* (2010:361),
– *skattebrottsdatalagen (2017:452),*	– *Kustbevakningens brottsdatalag (2012:145),*
– *tullbrottsdatalagen (2017:447),*	– *åklagarväsendets brottsdatalag (2015:433),*
– *kustbevakningsdatalagen* (*2012:145),*	– *Tullverkets brottsdatalag (2017:447),*
– *åklagardatalagen (2015:433),*	– *Skatteverkets brottsdatalag (2017:452),*
	– *Säkerhetspolisens datalag (2018:000), eller*
– förordningar som har stöd i dessa lagar, *eller*	– förordningar som har stöd i dessa lagar.

[2] Senaste lydelse 2017:456.

4. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

---

1. Denna lag träder i kraft den 1 maj 2018.
2. Äldre bestämmelser gäller fortfarande för uppgifter i handlingar som har omhändertagits för arkivering före ikraftträdandet av denna lag.

Bilaga 2

Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete[1]

Härigenom föreskrivs att 6 kap. 1 § lagen (2017:496) om internationellt polisiärt samarbete ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	1 §
Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller	Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller *följande författningar för respektive myndighet för behandling av personuppgifter vid internationellt polisiärt samarbete*
	– brottsdatalagen (2018:000), och
– polisdatalagen (2010:361) *för polisens behandling av personuppgifter vid internationellt polisiärt samarbete,*	*– polisens brottsdatalag* (2010:361),
– kustbevakningsdatalagen (2012:145) *för Kustbevakningens behandling av personuppgifter vid internationellt polisiärt samarbete, och*	*– Kustbevakningens brottsdatalag* (2012:145),
– tullbrottsdatalagen (2017:447) *för Tullverkets behandling av personuppgifter vid internationellt polisiärt samarbete.*	*– Tullverkets brottsdatalag (2017:447), eller*
	– Säkerhetspolisens datalag (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

[1] Observera att hänsyn inte har tagits till de förslag som lämnas i SOU 2017:29 s. 76.

Förteckning över remissinstanserna

Följande remissinstanser har kommit in med yttrande över SOU 2017:74 Brottsdatalag – kompletterande lagstiftning: Riksdagens ombudsmän, Svea hovrätt, Hovrätten för Västra Sverige, Södertörns tingsrätt, Eskilstuna tingsrätt, Helsingborgs tingsrätt, Umeå tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Linköping, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Övervakningsnämnd Stockholm Centrum, Brottsförebyggande rådet, Brottsoffermyndigheten, Rättsmedicinalverket, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Migrationsverket, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Försäkringskassan, Socialstyrelsen, Inspektionen för vård och omsorg, Statens institutionsstyrelse, Pensionsmyndigheten, Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Arbetsgivarverket, Länsstyrelsen Skåne, Länsstyrelsen Värmland, Länsstyrelsen Västernorrland, Avesta kommun, Hallstahammars kommun, Kiruna kommun, Luleå kommun, Norrköpings kommun, Sala kommun, Stockholms kommun, Statskontoret, Uppsala universitet, juridiska fakulteten, Umeå universitet, juridiska institutionen, Naturvårdsverket, Havs- och vattenmyndigheten, Post- och telestyrelsen, Sjöfartsverket, Riksarkivet, Sveriges advokatsamfund, Svenska Journalistförbundet, Tidningsutgivarna, Dataskydd.net, Svenska Fotbollförbundet och Riksidrottsförbundet.

Följande remissinstanser har avstått från att yttra sig respektive inte hörts av: Länsstyrelsen Stockholm, Blekinge läns landsting, Stockholms läns landsting, Västerbottens läns landsting, Alingsås kommun, Borgholms kommun, Danderyds kommun, Falu kommun, Göteborgs kommun, Helsingborgs kommun, Karlstads kommun, Laholms kommun, Lycksele kommun, Malmö kommun, Ronneby kommun, Sandvikens kommun, Sundsvalls kommun, Tierps kommun, Tranås kommun, Trelleborgs kommun, Uppsala kommun, Värnamo kommun, Växjö kommun, Åmåls kommun, Örebro kommun, Östersunds kommun, Sveriges Akademikers Centralorganisation (SACO), Landsorganisationen i Sverige (LO), Tjänstemännens centralorganisation (TCO), Svenskt Näringsliv, Sveriges Kommuner och Landsting (SKL), Sveriges Förenade Ordningsvakter, IT&Telekomföretagen, Civil Rights Defenders och Svenska Ishockeyförbundet.