Lagrådsremiss

Integritet och effektivitet i polisens brottsbekämpande verksamhet

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 5 november 2009

Beatrice Ask

Gunnel Lindberg
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Lagrådsremissen innehåller förslag till en ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Lagen ska ersätta polisdatalagen (1998:622). Lagen ska gälla i stället för personuppgiftslagen (1998:204) och innehålla hänvisningar till de bestämmelser i personuppgiftslagen som ska vara tillämpliga i polisens brottsbekämpande verksamhet.

Syftet med den nya lagen är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter i polisens brottsbekämpande verksamhet samt att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sådan verksamhet. En utgångspunkt är att skapa en teknikneutral och flexibel reglering som ger ramarna för polisens personuppgiftsbehandling utan att i detalj reglera formerna för behandlingen.

Genom den nya lagen kommer man till rätta med olika problem som den nuvarande regleringen har visat sig ge upphov till, bl.a. när det gäller möjligheterna att behandla personuppgifter för att förebygga, förhindra och upptäcka brottslig verksamhet. Den nya lagen skapar också förutsättningar för ett bättre samarbete mellan de brottsbekämpande myndigheterna genom utökade möjligheter till informationsutbyte.

Lagen reglerar, med några få undantag, all behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Personuppgiftsbehandling i sådan verksamhet som inte är brottsbekämpande, exempelvis hanteringen av förvaltningsärenden, omfattas inte av lagförslaget utan regleras liksom nu av personuppgiftslagen.

Polisen ska få behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Särskilda bestämmelser föreslås för sådan behandling som sker hos Säkerhetspolisen. För behandling av personuppgifter som fler än ett fåtal personer har åtkomst till (gemensamt tillgängliga uppgifter) föreslås olika begränsande bestämmelser för att värna den personliga integriteten. Ett fåtal register föreslås regleras särskilt i den nya lagen, bl.a. DNA-register och penningtvättsregister. Vidare föreslås en särskild lag som reglerar polisens allmänna spaningsregister.

Den externa tillsynen över polisens behandling av personuppgifter förstärks. Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden ska utöva sådan tillsyn.

Lagförslagen föreslås träda i kraft den 1 mars 2012.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
2. lag om polisens allmänna spaningsregister,
3. lag om ändring i rättegångsbalken,
4. lag om ändring i vapenlagen (1996:67),
5. lag om ändring i säkerhetsskyddslagen (1996:627),
6. lag om ändring i lagen (2000:344) om Schengens informationssystem,
7. lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet,
8. lag om ändring i offentlighets- och sekretesslagen (2009:400),
9. lag om ändring i offentlighets- och sekretesslagen (2009:400).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Härigenom föreskrivs följande.

1 kap. Lagens syfte och tillämpningsområde

Lagens syfte

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter i polisens brottsbekämpande verksamhet samt att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sådan verksamhet.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Lagen gäller inte vid behandling av personuppgifter enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2010:000) om polisens allmänna spaningsregister.

Lagen gäller inte heller när personuppgifter behandlas i vapenregister med stöd av vapenlagen (1996:67), om inte detta särskilt anges i den lagen.

3 § Följande bestämmelser gäller vid behandling av uppgifter om juridiska personer:

1. 2 kap. 7–9 §§ om ändamålen för behandlingen,
2. 2 kap. 11 § om tillgången till personuppgifter,
3. 2 kap. 12 och 13 §§ om bevarande och gallring,
4. 3 kap. 1–3, 9–12, 14 och 15 §§ om gemensamt tillgängliga uppgifter,
5. 4 kap. 18–20 §§ om behandling av personuppgifter i penningtvättsregister,
6. 4 kap. 21 och 22 §§ om behandling av personuppgifter i det internationella registret,
7. 5 kap. 1–3 §§ om ändamålen för behandlingen hos Säkerhetspolisen,
8. 5 kap. 4 § 5 om tillgången till personuppgifter hos Säkerhetspolisen,
9. 5 kap. 6 och 7 §§ om bevarande och gallring hos Säkerhetspolisen, och

10. 5 kap. 8, 9 och 12–14 §§ om gemensamt tillgängliga uppgifter hos Säkerhetspolisen.

Det som anges om personuppgifter i de angivna paragraferna ska därvid gälla för uppgifter om juridiska personer.

4 § I 2 kap. finns allmänna bestämmelser om behandling av personuppgifter.

För personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även bestämmelserna i 3 kap.

För personuppgifter som behandlas i register över DNA-profiler, fingeravtrycks- eller signalementsregister, penningtvättsregister eller i det internationella registret, gäller bestämmelser i 4 kap. i stället för bestämmelserna i 3 kap.

I 5 kap. finns bestämmelser om behandlingen av personuppgifter i Säkerhetspolisens verksamhet.

2 kap. Allmänna bestämmelser

Förhållandet till personuppgiftslagen

1 § Om inte annat anges i 2 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

2 § När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 §, med undantag för vad som anges i första stycket i och tredje stycket, om grundläggande krav på behandling,
4. 22 § om behandling av personnummer,
5. 23 och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
12. 48 § om skadestånd, och
13. 51 § första stycket, 52 § första stycket och 53 § om överklagande.

Om personuppgifter ska gallras enligt bestämmelser i denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller inte 8 § andra stycket personuppgiftslagen.

Information enligt 23 § personuppgiftslagen behöver inte lämnas vid behandling som består i insamling av personuppgifter genom bilder eller ljud. Sådan information behöver inte heller lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Definition av DNA-analys, DNA-profil och fingeravtryck

3 § I denna lag avses med

DNA-analys:	varje förfarande som kan användas för analys av deoxyribonukleinsyra i humant material,
DNA-profil:	resultatet av en DNA-analys som presenteras i form av siffror eller bokstäver, och
fingeravtryck:	fingeravtryck eller handavtryck.

Personuppgiftsansvar

4 § Rikspolisstyrelsen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför och den behandling som utförs i polisens verksamhet vid Ekobrottsmyndigheten. Var och en av polismyndigheterna är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

5 § Rikspolisstyrelsen och var och en av polismyndigheterna ska utse ett eller flera personuppgiftsombud.

Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Tillsyn

6 § Ytterligare bestämmelser om tillsyn finns i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Ändamål

7 § Personuppgifter får behandlas om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller beivra brott, eller
3. fullgöra de förpliktelser som följer av internationella åtaganden.

8 § Personuppgifter som behandlas enligt 7 §, får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,
3. sådan verksamhet hos polisen som avser handräckningsuppdrag,
4. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen,
5. verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten, eller
6. en myndighets verksamhet

a) om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift, eller

b) om tillhandahållandet görs i syfte att samverka mot brott.

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

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 7 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter och att uppgifter som behandlas i en förundersökning får tillhandahållas konkursförvaltare.

9 § Personuppgifter får behandlas om

1. det är nödvändigt för diarieföring, eller

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

Behandling av känsliga personuppgifter

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

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen. Uppgifter som avses i första stycket får också behandlas med stöd av 9 §.

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

Tillgången till personuppgifter

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

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om tillgången till personuppgifter.

Bevarande och gallring

12 § Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de i lagen angivna ändamålen.

I följande bestämmelser anges hur länge uppgifter som behandlas automatiserat längst får bevaras:

1. 13 § om uppgifter som inte har gjorts gemensamt tillgängliga,

2. 3 kap. 9–13 §§ om uppgifter i ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga,

3. 3 kap. 14 och 15 §§ om andra uppgifter som har gjorts gemensamt tillgängliga än som anges i 2,

4. 4 kap. 7 § om uppgifter i register över DNA-profiler,

5. 4 kap. 14–16 §§ om uppgifter i fingeravtrycks- eller signalementsregister,

6. 4 kap. 20 § om uppgifter i penningtvättsregister, och

7. 4 kap. 22 § om uppgifter i det internationella registret.

Regeringen meddelar föreskrifter om digital arkivering.

13 § Personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga eller behandlas i särskilda register enligt 4 kap. ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utlämnande av personuppgifter och uppgiftsskyldighet

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

15 § Om det är förenligt med svenska intressen, får personuppgifter lämnas till

1. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott, eller

2. utländsk underrättelse- eller säkerhetstjänst.

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

16 § Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Första stycket gäller inte uppgifter som behandlas i särskilda register enligt 4 kap.

17 § Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av uppgifter om huruvida personer förekommer

i register över DNA-profiler, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Uppgifter ur sådana register ska lämnas till Statens kriminaltekniska laboratorium, om myndigheten behöver uppgifterna i sin verksamhet.

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som behandlas i fingeravtrycks- eller signalementsregister enligt 4 kap. 11–17 §§, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Detsamma gäller Statens kriminaltekniska laboratorium, om myndigheten behöver uppgifterna i sin verksamhet.

19 § Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 14–18 §§.

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

Elektroniskt utlämnande av personuppgifter

20 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen meddelar föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall.

21 § Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag.

Regeringen meddelar föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, om detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 § samt 4 kap. 10 och 17 §§.

3 kap. Gemensamt tillgängliga uppgifter

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

Bestämmelserna i detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 9 §.

Personuppgifter som får göras gemensamt tillgängliga

2 § Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, om han eller hon

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra vad som följer av internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.

5. Uppgifter som har rapporterats till polisens kommunikationscentraler.

DNA-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

Särskilda upplysningar

3 § Vid behandling enligt 1 § ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska detta särskilt framgå.

4 § Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, 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 samband med misstänkt brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte detta på grund av särskilda omständigheter är onödigt. Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.

Sökning

5 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Det som anges i första stycket hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

6 § Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1,
4. övervakas enligt 2 § första stycket 2,
5. har anmält ett brott,
6. är målsägande i ett ärende som rör ansvar för brott,
7. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,
8. har gett in eller tillhandahållits en handling,
9. är anmäld såsom försvunnen,
10. har bedömts kunna komma att möta ett polisingripande med grovt våld, eller
11. är efterlyst.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om begränsning av tillgången till sådana uppgifter som avses i första stycket.

7 § Bestämmelsen i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller
2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Bestämmelsen i 6 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän och som görs

1. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, eller
2. för att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första och andra styckena.

Regeringen meddelar föreskrifter om ytterligare undantag från bestämmelserna i 6 §.

Direktåtkomst

8 § Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Bevarande av personuppgifter i ärenden om utredning eller beivrande av brott

9 § I 10–12 §§ anges hur länge personuppgifter i vissa ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga längst får bevaras i polisens brottsbekämpande verksamhet.

10 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas i polisens brottsbekämpande verksamhet efter det att åtal inte längre får väckas för brottet**.**

11 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då domen, eller det beslut som meddelades med anledning av talan, vann laga kraft.

Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

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

12 § Regeringen meddelar föreskrifter om att vissa kategorier av personuppgifter får bevaras i polisens brottsbekämpande verksamhet under längre tid än vad som anges i 10 och 11 §§.

13 § Om en förundersökning mot en person 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.

Bevarande och gallring av övriga personuppgifter

14 § Personuppgifter som har gjorts gemensamt tillgängliga enligt 2 § första stycket 1, 2, 4 eller 5 ska gallras enligt bestämmelserna i andra–sjätte styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Uppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver ska dock gallras

senast fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personen görs före utgången av gallringsfristen, behöver de uppgifter som finns om personen inte gallras så länge någon av uppgifterna om honom eller henne får bevaras.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Uppgifter som har behandlats med stöd av 2 § första stycket 4 ska gallras senast ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Uppgifter som har behandlats med stöd av 2 § första stycket 5 ska gallras senast ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Den tid då en misstänkt eller övervakad person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i andra och tredje styckena.

15 § Regeringen meddelar föreskrifter om att vissa kategorier av personuppgifter får bevaras under längre tid än vad som anges i 14 §.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 14 §, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

4 kap. Register

Register över DNA-profiler

Ändamål

1 § Rikspolisstyrelsen får föra register över DNA-profiler (DNA-registret, utredningsregistret och spårregistret) i enlighet med 2–10 §§. Dessa register får även föras för att underlätta identifiering av avlidna personer.

DNA-registret

2 § DNA-registret får innehålla DNA-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller
2. har godkänt ett strafföreläggande som avser villkorlig dom.

3 § En DNA-profil som registreras får endast ge information om identitet och inte om personliga egenskaper.

Utöver DNA-profiler får DNA-registret innehålla uppgifter om vem analysen avser och i vilket ärende DNA-profilen har tagits fram samt brottskod.

Utredningsregistret

4 § Utredningsregistret får innehålla DNA-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket fängelse kan följa.

Bestämmelserna i 3 § gäller också vid registrering i utredningsregistret.

Spårregistret

5 § Spårregistret får innehålla DNA-profiler som har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver DNA-profiler får spårregistret innehålla upplysningar som visar i vilket ärende analysen har gjorts och brottskod.

6 § DNA-profiler i spårregistret får jämföras med DNA-profiler

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

DNA-profiler i spårregistret får också jämföras i andra fall om det är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Gallring

7 § Uppgifter i DNA-registret ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i utredningsregistret ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter i spårregistret ska gallras senast trettio år efter registreringen. Sådana uppgifter ska dock gallras senast sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om

1. mord eller dråp enligt 3 kap. 1 eller 2 § brottsbalken,
2. folkrättsbrott enligt 22 kap. 6 § andra stycket brottsbalken,
3. folkmord enligt 1 § lagen (1964:169) om straff för folkmord,
4. terroristbrott enligt 3 § 1 eller 2 jämförd med 2 § lagen (2003:148) om straff för terroristbrott, eller
5. försök till brott som avses i 1, 3 eller 4.

Prover för DNA-analys

8 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys, får provet inte användas för något annat ändamål än det som provet togs för.

9 § Ett prov för DNA-analys som har tagits med stöd av 28 kap. rättegångsbalken, eller på begäran av en annan stat, ska förstöras senast sex månader efter det att provet togs.

Direktåtkomst

10 § Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Statens kriminaltekniska laboratorium får medges direktåtkomst till register över DNA-profiler.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Fingeravtrycks- eller signalementsregister

Ändamål

11 § Rikspolisstyrelsen får föra fingeravtrycks- eller signalementsregister i enlighet med 12–17 §§. Dessa register får även föras för att underlätta identifiering av okända personer.

Innehåll

12 § I fingeravtrycks- eller signalementsregister får uppgifter behandlas om en person som

1. är misstänkt eller dömd för brott och som har varit föremål för åtgärd enligt 28 kap. 14 § rättegångsbalken, eller
2. har lämnat fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll.

Uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person får behandlas om uppgiften kommit fram i en utredning om brott.

Uppgifter om fingeravtryck får även behandlas om det behövs för att fullgöra internationella åtaganden.

I fingeravtrycks- eller signalementsregister får inte uppgifter behandlas som har lämnats av en person under femton år enligt 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

13 § Fingeravtrycks- eller signalementsregister får innehålla uppgifter om

1. fingeravtryck,
2. signalement,
3. fotografi,
4. videoupptagning,
5. identifieringsuppgifter,
6. ärendenummer, och
7. brottskod.

Gallring

14 § Uppgifter i fingeravtrycks- eller signalementsregister om en misstänkt person ska gallras senast tre månader efter att uppgifter om personen gallrats ur misstankeregistret som förs enligt lagen (1998:621) om misstankeregister och ur belastningsregistret som förs enligt lagen (1998:620) om belastningsregister.

Uppgifter som inte kan hänföras till en identifierbar person ska gallras senast trettio år efter registreringen. Sådana uppgifter ska dock gallras senast sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om

1. mord eller dråp enligt 3 kap. 1 eller 2 § brottsbalken,
2. folkrättsbrott enligt 22 kap. 6 § andra stycket brottsbalken,
3. folkmord enligt 1 § lagen (1964:169) om straff för folkmord,
4. terroristbrott enligt 3 § 1 eller 2 jämförd med 2 § lagen (2003:148) om straff för terroristbrott, eller
5. försök till brott som avses i 1, 3 eller 4.

15 § Uppgifter i fingeravtrycks- eller signalementsregister som behandlas för att fullgöra ett internationellt åtagande ska gallras när uppgifterna inte längre behövs för ändamålet med behandlingen.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll ska gallras senast tio år efter registreringen.

16 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 14 och 15 §§, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Direktåtkomst

17 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen, Skatteverket och Statens kriminaltekniska laboratorium får medges direktåtkomst till personuppgifter i fingeravtrycks- eller signalementsregister.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Penningtvättsregister

Ändamål

18 § Rikspolisstyrelsen får behandla personuppgifter i penningtvättsregister om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet

1. där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller
2. som innefattar finansiering av terrorism.

19 § I ett penningtvättsregister får personuppgifter behandlas som
1. kan antas ha samband med sådan brottslig verksamhet som avses i 18 §,
2. har rapporterats till Rikspolisstyrelsen med stöd av bestämmelser i lag eller annan författning, eller
3. har lämnats av en utländsk myndighet som i sin stat ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i 18 §.

Gallring

20 § Personuppgifter i ett penningtvättsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Det internationella registret

Ändamål

21 § Rikspolisstyrelsen får behandla personuppgifter i det internationella registret om det behövs för handläggningen av ärenden som rör internationellt polisiärt samarbete eller internationellt straffrättsligt samarbete.

Uppgifter angående dödsfall, olyckshändelser eller andra liknande händelser i utlandet får också behandlas i det internationella registret, om ärendet rör en fråga som ska handläggas av polisen.

Gallring

22 § Personuppgifter i det internationella registret ska gallras senast tre år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

5 kap. Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

Ändamål

1 § Personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
   a) brott mot rikets säkerhet,
   b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,
   c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, eller
   d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,
2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra uppgifter i samband med personskydd,
4. fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627),
5. fullgöra de förpliktelser som följer av internationella åtaganden, eller
6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

2 § Personuppgifter som behandlas enligt 1 §, får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. en myndighets verksamhet, om tillhandahållandet görs i syfte att samverka mot brott,
3. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller
4. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation.

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

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 1 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter.

3 § Personuppgifter får behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Tillämpliga bestämmelser i 2 kap.

4 § Följande bestämmelser i 2 kap. ska tillämpas vid behandling av personuppgifter hos Säkerhetspolisen:

1. 1 och 2 §§ om förhållandet till personuppgiftslagen (1998:204),
2. 3 § om definition av DNA-analys, DNA-profil och fingeravtryck,
3. 6 § om tillsyn,
4. 10 § om behandling av känsliga personuppgifter,
5. 11 § om tillgången till personuppgifter,
6. 14, 15 och 19 §§ om utlämnande av personuppgifter och uppgiftsskyldighet, och
7. 20 och 21 §§ om elektroniskt utlämnande av personuppgifter.

Personuppgiftsansvar

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

Säkerhetspolisen ska utse ett eller flera personuppgiftsombud. Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Bevarande och gallring

6 § Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av ändamålen i 1–3 §§.

I 7 och 12–14 §§ anges hur länge uppgifter som behandlas automatiserat längst får bevaras.

Regeringen meddelar föreskrifter om digital arkivering.

7 § Personuppgifter som behandlas automatiserat hos Säkerhetspolisen och som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Behandling av gemensamt tillgängliga uppgifter

Gemensamt tillgängliga uppgifter

8 § Om det behövs för de ändamål som anges i 1 §, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet. Detta gäller dock inte DNA-profiler. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Bestämmelserna i 9–13 §§ gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Bestämmelserna gäller dock inte när personuppgifter behandlas med stöd av 3 §.

Särskilda upplysningar

9 § Vid behandling enligt 8 § ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas.

10 § Om uppgifter, som behandlas enligt 8 §, 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.

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. Sådan upplysning behöver dock inte lämnas, om det på grund av särskilda omständigheter är onödigt. Någon upplysning 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 och analysen befinner sig i ett inledande skede.

Sökning

11 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som anges i 1 §.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om sökning i gemensamt tillgängliga uppgifter.

Bevarande och gallring

12 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en sådan uppgiftssamling som avses i 10 § andra stycket 1 ska dock 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 än vad som anges i första och andra styckena, om uppgifterna fortfarande behövs för det ändamål som de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i

andra stycket, senast vid utgången av det tredje kalenderåret efter beslutet.

13 § Bestämmelserna i 12 § gäller inte personuppgifter i ärenden om utredning eller beivrande av brott. I fråga om behandling av sådana personuppgifter ska i stället 3 kap. 9–13 §§ tillämpas.

14 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 12 §, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

---

1. Denna lag träder i kraft den 1 mars 2012, då polisdatalagen (1998:622) upphör att gälla.

2. För signalements- och kännetecknsregistret och det centrala brottsspaningsregistret som förs med stöd av punkt 2 i övergångsbestämmelserna till polisdatalagen (1998:622) gäller bestämmelserna i datalagen (1973:289) i stället för bestämmelserna i denna lag till utgången av år 2014. Bestämmelserna i 2 kap. 14, 15 och 19 §§ i denna lag ska dock tillämpas på uppgifterna i registren från lagens ikraftträdande.

3. Datainspektionens tillstånd att föra de register som anges i punkt 2 upphör att gälla vid utgången av år 2014 eller vid den tidigare tidpunkt då den personuppgiftsansvarige avanmäler registret hos inspektionen. Vid ikraftträdandet av denna lag upphör Datainspektionens tillstånd för övriga register som förs med stöd av punkt 2 i övergångsbestämmelserna till polisdatalagen (1998:622) att gälla.

4. I fråga om behandling av personuppgifter i en särskild undersökning enligt 14 § första stycket 1 polisdatalagen (1998:622), som har beslutats före ikraftträdandet av denna lag, gäller bestämmelserna i polisdatalagen i stället för bestämmelserna i denna lag till utgången av år 2014.

5. Följande bestämmelser i denna lag behöver inte tillämpas förrän den 1 januari 2015

a) 3 kap. 4 § första stycket om särskilda upplysningar, när det gäller annan verksamhet än sådan som bedrivs för ändamål som anges i 2 kap. 7 § 1,

b) 3 kap. 6 och 7 §§ om sökning, och

c) 3 kap. 10, 11 och 13 §§ om behandling av personuppgifter i brottsanmälningar, avslutade förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

6. Bestämmelsen i 3 kap. 4 § andra stycket i denna lag om särskilda upplysningar behöver inte tillämpas på uppgifter som har samlats in före ikraftträdandet.

2.2 Förslag till lag om polisens allmänna spaningsregister

Härigenom föreskrivs följande.

Allmänt spaningsregister

1 § Rikspolisstyrelsen får med hjälp av automatiserad behandling föra ett allmänt spaningsregister.

Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Förhållandet till personuppgiftslagen

2 § Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter i det allmänna spaningsregistret, om inte annat följer av denna lag eller av föreskrifter som har meddelats i anslutning till denna lag.

Ändamål

3 § Det allmänna spaningsregistret ska ha till ändamål att utgöra underlag för systematisering av vissa personuppgifter som framkommit i polisens brottsbekämpande verksamhet. Registret får föras för att underlätta tillgången till sådan information som behövs i polisens spaningsverksamhet.

4 § Personuppgifter i registret får behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,
3. sådan verksamhet hos polisen som avser handräckningsuppdrag, eller
4. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen.

Personuppgifter får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. I övrigt gäller 9 § första stycket d personuppgiftslagen (1998:204).

Innehåll

5 § I registret får uppgifter om en person behandlas, om

1. den som uppgiften avser kan misstänkas för ett brott som inte har enbart böter i straffskalan, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

6 § I registret får uppgifter om en person som inte kan misstänkas för brott behandlas, om

1. uppgiften har samband med en person som har registrerats enligt 5 §, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

7 § Utöver de uppgifter som får behandlas enligt 5 och 6 §§, får uppgifter behandlas om en juridisk person eller ett transportmedel eller annat föremål som kan hänföras till en fysisk person, om

1. uppgiften kan antas ha samband med ett brott som inte har enbart böter i straffskalan, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

8 § Registret ska innehålla uppgifter om

1. grunden för att en person registreras som misstänkt enligt 5 § eller att uppgifter om en juridisk person, ett transportmedel eller föremål enligt 7 § förs in i registret och omständigheterna i samband med registreringen,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än sådana som avses i 1 tillförs registret, och
3. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

En upplysning enligt första stycket 3 behöver inte lämnas om det på grund av särskilda omständigheter är onödigt.

9 § Registret får, utöver vad som anges i 8 §, innehålla följande uppgifter om en person som har registrerats enligt 5 §:

1. uppgift som är ägnad att identifiera personen, dock inte DNA-profil eller fingeravtryck,
2. uppgift om vistelseadress,
3. uppgift om verkställighet av påföljd för brott,
4. uppgift om att personen är eftersökt i samband med brott,
5. uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
6. uppgift om att personen är föremål för sådan övervakning som avses i 3 kap. 2 § första stycket 2 lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
7. uppgift om anknytning till juridisk person,
8. uppgift om anknytning till andra personer som har registrerats enligt 5 § och som kan antas tillhöra samma gruppering som den registrerade,
9. uppgift om att personen har använt något speciellt tillvägagångssätt, och
10. ärendenummer.

10 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får behandlas i registret och om förfarandet vid registreringen.

Särskilda upplysningar

11 § Vid behandling av uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Behandling av känsliga personuppgifter

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

Om uppgifter om en person behandlas på annan grund, får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen.

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

Tillgången till personuppgifter

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

Sökning

14 § Vid sökning i registret får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Det som anges i första stycket hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

15 § Uppgifter i registret som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara.

Utlämnande av personuppgifter och uppgiftsskyldighet

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

17 § Om det är förenligt med svenska intressen, får personuppgifter lämnas till

1. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott, eller
2. en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av uppgifter i registret, om myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Regeringen meddelar föreskrifter om att uppgifter får lämnas ut i andra fall än som anges i första stycket.

Bestämmelser om att uppgifter får lämnas ut finns även i offentlighets- och sekretesslagen.

Elektroniskt utlämnande av personuppgifter

19 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen meddelar föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall.

20 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till registret.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Gallring

21 § Uppgifter om en person som har registrerats enligt 5 § ska gallras senast tre år efter det att uppgiften om misstanke om brott registrerades. Om uppgiften avser misstanke om brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver uppgifterna inte gallras förrän fem år efter registreringen.

Om en ytterligare uppgift om personen förs in i registret, förlängs gallringsfristen med

1. fem år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. tre år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om annat brott än som anges i 1, eller
3. ett år från det att den nya uppgiften fördes in i registret, om uppgiften inte avser misstanke om brott.

Den tid då en person som har registrerats enligt 5 § avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i första och andra styckena.

22 § Uppgifter om en person som avses i 6 § ska gallras senast när uppgifterna om den person som har registrerats enligt 5 § och som uppgifterna har samband med gallras.

23 § Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats enligt 7 § ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver uppgifterna inte gallras förrän fem år efter det att den senaste uppgiften infördes.

24 § Om det finns synnerliga skäl, får regeringen, eller den myndighet som regeringen bestämmer, i ett enskilt fall besluta att en uppgift får bevaras under längre tid än vad som anges i 21–23 §§. Ett sådant beslut ska omprövas varje år.

25 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om gallring.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 21–23 §§, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Rättelse och skadestånd

26 § Bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen.

---

1. Denna lag träder i kraft den 1 mars 2012 och gäller till och med den 28 februari 2017.

2. Bestämmelserna i 8 § första stycket 3 i denna lag behöver inte tillämpas på uppgifter som har samlats in före ikraftträdandet.

2.3 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 28 kap. 12 a och 12 b §§ rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
28 kap.	
12 §[1]	
Kroppsbesiktning genom tagande av salivprov får *ske* på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera *uppgifter om resultatet av analysen* i det DNA-register eller det utredningsregister som förs enligt *polisdatalagen (1998:622)*.	Kroppsbesiktning genom tagande av salivprov får *göras* på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera *DNA-profilen* i det DNA-register eller det utredningsregister som förs enligt *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.*
12 b §[2]	
Kroppsbesiktning genom tagande av salivprov får *ske* på annan än den som skäligen kan misstänkas för ett brott, om	Kroppsbesiktning genom tagande av salivprov får *göras* på annan än den som skäligen kan misstänkas för ett brott, om
1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och	
2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.	
Analysresultatet får inte jämföras med de *uppgifter* som finns registrerade i *register* som förs enligt *polisdatalagen (1998:622)* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.	Analysresultatet får inte jämföras med de *DNA-profiler* som finns registrerade i register över DNA-profiler som förs enligt *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.
Första stycket gäller inte den som är under 15 år.	

Denna lag träder i kraft den 1 mars 2012.

[1] Senaste lydelse 2005:878.
[2] Senaste lydelse 2005:878.

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

Härigenom föreskrivs att det i vapenlagen (1996:67) ska införas en ny paragraf, 2 kap. 22 §, samt närmast före 2 kap. 22 § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	Utlämnande av personuppgifter och uppgiftsskyldighet
	22 § *Bestämmelserna om utlämnande av personuppgifter och uppgiftsskyldighet i 2 kap. 14 och 15 §§ lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet gäller även när personuppgifter behandlas i vapenregister enligt denna lag.* *Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut även i andra fall.*

Denna lag träder i kraft den 1 mars 2012.

2.5 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12, 21 och 22 §§ 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 misstankeregister *eller polisdatalagen (1998:622).* Med registerkontroll avses också att *sådana personuppgifter* hämtas som *Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild undersökning i kriminalunderrättelseverksamhet.*	Med registerkontroll avses att uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister *eller lagen (2010:000) om polisens allmänna spaningsregister*. Med registerkontroll avses också att *uppgifter* hämtas som *behandlas med stöd av lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.*
21 §[2]	
Utlämnande av uppgifter vid registerkontroll får omfatta	
1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och	
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret, misstankeregistret, *SÄPO-registret och* uppgifter som *annars* behandlas hos Säkerhetspolisen.	2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.
22 §[3]	
Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret, misstankeregistret, *SÄPO-registret och*	Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret *och* misstankeregistret *samt* uppgifter

[1] Senaste lydelse 1998:625.
[2] Senaste lydelse 1998:625.
[3] Senaste lydelse 2006:347.

uppgifter som *annars* behandlas hos Säkerhetspolisen.	som behandlas hos Säkerhetspolisen.

Denna lag träder i kraft den 1 mars 2012.

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

Härigenom föreskrivs att 5 § lagen (2003:344) om Schengens informationssystem ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §
Registret *skall* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.	Registret *ska* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.
Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen (1998:622)* eller annan svensk författning.	Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller annan svensk författning.

Denna lag träder i kraft den 1 mars 2012.

2.7 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.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden (nämnden) *skall* utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.	Säkerhets- och integritetsskyddsnämnden (nämnden) *ska* utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.
Nämnden *skall* även utöva tillsyn över *Säkerhetspolisens* behandling av *uppgifter* enligt *polisdatalagen (1998:622), särskilt med avseende på 5 § den lagen.*	Nämnden *ska* även utöva tillsyn över *polisens* behandling av *personuppgifter* enligt *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lagen (2010:000) om polisens allmänna spaningsregister. Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och 12 § lagen om polisens allmänna spaningsregister.*
Tillsynen *skall* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.	Tillsynen *ska* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Denna lag träder i kraft den 1 mars 2012.

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

Härigenom föreskrivs att 18 kap. 18 § och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
18 §	
Sekretessen enligt 17 § hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i polisdatalagen (1998:622) och lagen (2000:344) om Schengens informationssystem.	Sekretessen enligt 17 § *andra stycket* hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i polisdatalagen (1998:622) och lagen (2000:344) om Schengens informationssystem.
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 denne 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, en polismyndighet, Skatteverket, Statens kriminaltekniska laboratorium, Tullverket eller Kustbevakningen,	
5. Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller en polismyndighet i brottmål,	
6. register som förs av Rikspolisstyrelsen enligt polisdatalagen (1998:622) eller som annars behandlas där med stöd av samma lag,	
7. register som förs enligt lagen (1998:621) om misstankeregister,	
8. register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,	
9. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i *4 kap.* 1 §, eller	9. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i *5 kap.* 1 §, eller

10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet 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 denne 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 denne 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.

Denna lag träder i kraft den 1 juli 2010.

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

Härigenom föreskrivs att 18 kap. 2 och 18 §§, 35 kap. 1 och 10 §§ samt 37 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
2 §	
Sekretess gäller för uppgift som hänför sig till sådan *underrättelseverksamhet* som avses i *3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott*, 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. 7 § 1 eller 5 kap. 1 § 1 lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet*, 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

1. sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, eller
2. sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

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 lagförslag i avsnitt 2.8	*Föreslagen lydelse*
18 §	
Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622) och* lagen (2000:344) om Schengens informationssystem.	Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem *och lagen (2010:000) om behand-*

ling av personuppgifter i polisens brottsbekämpande verksamhet.

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 denne 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, en polismyndighet, Skatteverket, Statens kriminaltekniska laboratorium, Tullverket eller Kustbevakningen,

5. Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller en polismyndighet i brottmål,

6. register som förs av Rikspolisstyrelsen enligt *polisdatalagen (1998:622)* eller som annars behandlas där med stöd av samma lag,

6. register som förs av Rikspolisstyrelsen enligt *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller som annars behandlas där med stöd av samma lag,

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

8. register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

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

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

10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag.

10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag, *eller*

11. register som förs enligt lagen (2010:000) 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 denne 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 denne 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 §	
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,	
3. enligt vad som föreskrivs i	3. enligt vad som föreskrivs i
– lagen (1998:621) om misstankeregister,	– lagen (1998:621) om misstankeregister,
– *polisdatalagen (1998:622),*	– *lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,*
– lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar,	– lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar,
– lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet,	– lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet,
– förordningar som har stöd i dessa lagar, eller	– förordningar som har stöd i dessa lagar, eller
4. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.	

37 kap.

7 §	
Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622) och* lagen (2000:344) om Schengens informationssystem.	Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem *och lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet*.

---

1. Denna lag träder i kraft den 1 mars 2012.

2. Äldre bestämmelser gäller fortfarande för uppgifter i sådana ärenden där handlingar omhändertagits för arkivering före denna tidpunkt.

3 Ärendet och dess beredning

Polisdatalagen (1998:622), som trädde i kraft den 1 april 1999, innehåller bestämmelser om behandling av personuppgifter hos polisen. Den innehåller de särskilda regler som, utöver bestämmelserna i personuppgiftslagen (1998:204), har ansetts nödvändiga i polisens verksamhet. För frågor som inte regleras i polisdatalagen gäller således personuppgiftslagen. Polisdatalagen utgör emellertid bara en del av den lagstiftning som reglerar behandlingen av personuppgifter i polisens verksamhet. Andra lagar som reglerar sådan behandling är bl.a. lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister. En stor del av den behandling av personuppgifter som sker hos polisen är dock inte författningsreglerad. Enligt övergångsbestämmelserna till polisdatalagen gäller den upphävda datalagen (1973:289) och Datainspektionens tillstånd fortfarande för de register som den 24 oktober 1998 fördes med Datainspektionens tillstånd. Detta gäller flera av de stora polisregistren, t.ex. det allmänna spaningsregistret. Övergångsbestämmelserna, som har förlängts flera gånger (senast genom SFS 2008:880), gäller till utgången av år 2009. I propositionen Övergångsbestämmelserna till polisdatalagen (1998:622) har föreslagits ytterligare förlängning av övergångsbestämmelserna till utgången av juni 2012 (prop. 2009/10:23).

Den 9 december 1999 tillkallade den dåvarande regeringen en särskild utredare med uppdrag att följa genomförandet av den nya polisregisterlagstiftningen och påtala eventuella brister i regelverket. Utredaren skulle överväga om det behövde vidtas några åtgärder för att lagstiftningen skulle uppnå sitt syfte att skapa en effektiv brottsbekämpning och samtidigt värna om den enskildes personliga integritet. Utredningen antog namnet Polisdatautredningen.

I november 2001 överlämnade utredningen betänkandet Behandling av personuppgifter i polisens verksamhet (SOU 2001:92). En sammanfattning av betänkandet finns i *bilaga 1*. Utredningens lagförslag har tagits in i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. En remissammanställning finns tillgänglig i Justitiedepartementet (dnr Ju2001/8624/PO).

Remissinstanserna godtog i allmänhet Polisdatautredningens förslag att polisdatalagen skulle ersättas med en helt ny reglering. I fråga om enskildheter i förslaget var dock remissynpunkterna mera blandade. Flera remissinstanser efterlyste en närmare analys av olika delar av förslaget. Under den fortsatta beredningen av ärendet framkom att förslaget behövde ändras och kompletteras i flera olika avseenden. Inom Justitiedepartementet utarbetades därför departementspromemorian Behandling av personuppgifter i polisens brottsbekämpande verksamhet (Ds 2007:43). Promemorians lagförslag har tagits in i *bilaga 4*. Promemorian har remitterats. En förteckning över remissinstanserna finns i *bilaga 5*. En sammanställning av remissyttrandena finns tillgänglig i Justitiedepartementet (dnr Ju2007/9805/PO).

Den del av promemorian som rör en framställan från Kustbevakningen om att myndigheten i sin brottsbekämpande verksamhet ska få tillgång till uppgifter i belastningsregistret och misstankeregistret genom direktåt-

komst (dnr Ju2005/319/PO) har behandlats i propositionen Några frågor om sekretess och tillgång till register (prop. 2008/09:152).

Inom Regeringskansliet (Försvarsdepartementet) pågår ett arbete med att ta fram ett förslag till en lag om Kustbevakningens behandling av personuppgifter. Avsnittet i promemorian om Kustbevakningens personuppgiftsbehandling bereds inom ramen för det lagstiftningsarbetet. Frågan kommer således inte att behandlas i detta lagstiftningsärende.

Regeringen gav den 29 januari 2009 Rikspolisstyrelsen i uppdrag att bl.a. inventera de digitala register, ärendehanteringssystem och uppgiftssamlingar som helt eller delvis förs med stöd av polisdatalagen eller dess övergångsbestämmelser och som omfattas av förslagen i departementspromemorian med förslag till ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Inventeringen skulle även omfatta nya datasystem som planeras att tas i bruk under de närmaste två åren (dnr Ju2009/889/PO). I uppdraget ingick att redovisa vilka av datasystemen som inte utan förändringar skulle kunna föras med stöd av förslagen i departementspromemorian. Rikspolisstyrelsen redovisade uppdraget i denna del den 14 april 2009 (dnr Ju2009/3375/PO).

Inom ramen för Rådet för rättsväsendets informationsförsörjning (RIF-rådet), som består av elva myndigheter i den s.k. rättskedjan, bedrivs ett arbete för att skapa ett elektroniskt informationsflöde som möjliggör att viss information kan återanvändas av andra myndigheter i rättskedjan. En sådan ordning innebär stora effektivitetsvinster. Arbetet syftar till att införa en helt elektronisk ärendehantering. Härigenom blir det möjligt att följa ett ärende från polisanmälan till verkställd dom. Det skapar bl.a. möjlighet att få en elektronisk återkoppling till polisen om en brottsutredning har lett till dom eller inte. Regeringen har beslutat att RIF-rådet från den 15 mars 2009 ska ledas från Regeringskansliet genom expeditionschefen vid Justitiedepartementet. Arbetet, som har intensifierats särskilt vad gäller informationsflödet och samarbetet mellan polisen, åklagarväsendet, Domstolsverket, Kriminalvården och Brottsförebyggande rådet, har praktisk betydelse för hur polisen ska bygga sitt nya IT-stöd.

4 Gällande rätt och internationella överenskommelser

4.1 Inledning

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. I 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. I 2 kap. 3 § andra stycket sägs att varje medborgare, i den utsträckning som anges i lag, ska skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Den sistnämnda bestämmelsen

riktar sig framför allt till den lagstiftande makten, som har att bevaka att den enskilde ges erforderligt skydd i berört hänseende.

Personuppgiftslagen (1998:204) är den lag som har till syfte att i första hand uppfylla vad regeringsformen föreskriver i fråga om integritetsskydd vid automatiserad personuppgiftsbehandling. Lagen trädde i kraft den 24 oktober 1998. Genom lagen genomfördes Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet) i svensk rätt. Personuppgiftslagen är tillämplig, om det inte i någon annan lag eller förordning har meddelats avvikande bestämmelser. Då gäller dessa. Direktivet omfattar däremot inte all personuppgiftsbehandling. Verksamhet som rör allmän säkerhet och statens verksamhet på straffrättens område omfattas t.ex. inte.

Sedan slutet av 1990-talet har det utöver personuppgiftslagen utarbetats en stor mängd specialförfattningar med bestämmelser om behandling av personuppgifter, däribland polisdatalagen (1998:622). Syftet har varit att anpassa lagstiftningen till de särskilda behov som finns inom olika verksamhetsområden och samtidigt göra avvägningar mellan behovet av effektivitet i berörd verksamhet och behovet av skydd för enskildas integritet.

Utöver en beskrivning av gällande rätt innehåller detta kapitel en redogörelse för aktuella internationella överenskommelser och rekommendationer på dataskyddsområdet. Dessa instrument utgör en utgångspunkt för en ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Vidare redovisas några nyligen antagna beslut inom Europeiska unionen (EU) som rör informationsutbyte mellan medlemsstaterna.

4.2 Internationella överenskommelser och personuppgiftslagen

4.2.1 Europakonventionen och FN-konventionen om medborgerliga och politiska rättigheter

År 1948 antog Förenta nationerna (FN) den allmänna förklaringen om de mänskliga rättigheterna. De rättigheter som räknas upp i förklaringen har därefter vidareutvecklats bl.a. i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) från år 1950 och FN:s konvention om medborgerliga och politiska rättigheter från år 1966.

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt bl.a. för sitt privat- och familjeliv. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

I kriteriet ”med stöd av lag” ligger, utöver att intrånget ska ha stöd i nationell lag, att den åberopade lagen måste uppfylla vissa minimikrav i fråga om kvalitet och tydlighet. En rättighetsinskränkande tolkning av lagen ska kunna förutses och lagen ska vara allmänt tillgänglig. De syften för vilka intrång tillåts har tolkats ganska extensivt av Europadomstolen, men domstolen avgör också vad som kan anses nödvändigt för att tillgodose ett i och för sig legitimt syfte. Hela konventionen genomsyras av att åtgärder som innefattar intrång i en skyddad rättighet kan godtas endast om de är proportionerliga. Det innebär att intrånget måste svara mot ett angeläget samhällsbehov och stå i rimlig proportion till det syfte som ska uppnås.

I artikel 13 i Europakonventionen föreskrivs att var och en, vars i konventionen angivna fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller även om kränkningen förövats av någon under utövning av offentlig myndighet. Innebörden av artikeln är att den enskilde ska ha tillgång till en nationell instans för att kunna få saken prövad och kunna få rättelse. Prövningen kan utföras av domstol, men något krav på domstolsprövning uppställs inte. Prövning av en stats regering eller av en förvaltningsmyndighet kan vara tillräckligt för att uppfylla konventionens krav på tillgång till ett effektivt rättsmedel.

Även i FN:s konvention om medborgerliga och politiska rättigheter finns en bestämmelse till skydd för godtyckligt eller olagligt ingripande i någons privat- och familjeliv (artikel 17).

4.2.2 Dataskyddskonventionen m.m.

Bestämmelser av betydelse för automatisk databehandling av personuppgifter finns också i Europarådets konvention från år 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Dataskyddskonventionen trädde i kraft den 1 oktober 1985. Samtliga medlemsstater i EU har ratificerat konventionen.

Dataskyddskonventionens innehåll kan ses som en precisering av skyddet enligt artikel 8 i Europakonventionen för enskilda vid automatisk databehandling. Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med behandling av personuppgifter och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

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

Vissa typer av personuppgifter får, enligt konventionen, behandlas endast om den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörig-

het, religiös tro eller övertygelse i övrigt, hälsa, sexualliv samt uppgifter om brott.

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

Dataskyddskonventionens roll som grundläggande dokument för automatiserad behandling av personuppgifter inom EU har i princip övertagits av dataskyddsdirektivet (avsnitt 4.2.5). Direktivet omfattar dock inte behandling av personuppgifter inom områden som allmän säkerhet, försvar och statens säkerhet. På dessa områden är dataskyddskonventionen således fortfarande av betydelse.

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

Även Organisationen för ekonomiskt samarbete och utveckling (OECD) har utarbetat internationella riktlinjer om integritetsskydd och persondataflöde över gränserna. Ett antal internationella organisationer och företag har antagit egna regler om dataskydd som bygger på OECD:s riktlinjer. Riktlinjerna motsvarar i princip de bestämmelser som finns i dataskyddskonventionen.

4.2.3 Europarådets rekommendation för polissektorn

Utöver dataskyddskonventionen har Europarådet tagit fram sektorsvisa rekommendationer om dataskydd, bl.a. en rekommendation, No. R (87) 15, som reglerar användningen av personuppgifter inom polissektorn. Rekommendationen innehåller speciella skyddsregler för personuppgifter som polisen samlar in, lagrar, använder eller överför med hjälp av automatiserad behandling i syfte att förhindra och bekämpa brott eller upprätthålla allmän ordning. Endast sådana uppgifter som är nödvändiga för att förhindra en verklig fara eller bekämpa ett visst brott får samlas in, om inte den nationella lagstiftningen tillåter ett mer omfattande uppgiftssamlande. Olika kategorier av lagrade uppgifter ska så långt som möjligt kunna skiljas från varandra efter graden av riktighet och tillförlitlighet. I synnerhet ska uppgifter som grundar sig på fakta kunna skiljas från uppgifter som grundar sig på omdömen eller personliga värderingar.

4.2.4 Europeiska unionens stadga om de grundläggande rättigheterna

Den 7 december 2000 tillkännagavs Europeiska unionens stadga om de grundläggande rättigheterna av parlamentet, rådet och kommissionen. I stadgan bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser samt i Fördraget om Europeiska unionen och gemenskapsfördragen. Stadgans syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner. För närvarande är stadgan endast en viljeförklaring avseende de redan existerande rättigheterna.

I stadgan föreskrivs bl.a. att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs. Stadgan avser endast verksamhet som utförs av EU:s egna organ och institutioner och blir tillämplig för medlemsstaterna endast i de fall de tillämpar EG-rätten. Stadgan är följaktligen inte tillämplig på nationell lagstiftning inom områden där EU inte har lagstiftningskompetens.

När det gäller de garanterade rättigheternas räckvidd anförs i stadgan att varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och vara förenlig med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. Hänvisning görs också till de grundläggande fördragen och Europakonventionen. De rättigheter som skyddas i stadgan ska ha samma innebörd och räckvidd som de som skyddas i konventionen. Stadgans artiklar får inte tolkas som att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter.

4.2.5 Dataskyddsdirektivet och personuppgiftslagen

Dataskyddsdirektivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Medlemsstaterna får inom den ram som anges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Sådana preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen. Direktivet gäller inte för sådan behandling av personuppgifter som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Direktivet omfattar således inte statens behandling av personuppgifter i brottsbekämpande verksamhet. Denna fråga kommer att behandlas närmare i avsnitt 6.4.1.

Personuppgiftslagen, genom vilken dataskyddsdirektivet genomförts i svensk rätt, har emellertid gjorts generellt tillämplig och omfattar således även sådan verksamhet som faller utanför direktivets tillämpningsområde

(prop. 1997/98:44, bet. 1997/98:KU18). Lagen trädde i kraft den 24 oktober 1998 och innehåller de generella regler som krävs för genomförandet av direktivet. Lagen anger den grundläggande ramen för behandling av personuppgifter. Särreglering i lag eller förordning gäller emellertid framför bestämmelserna i personuppgiftslagen. Att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger, är en garanti för att behovet av särregler övervägs noga i den ordning som gäller för författningsgivning.

Tidigare fanns det grundläggande regler om inrättande och förande av personregister med hjälp av automatisk databehandling i datalagen (1973:289), som upphävdes när personuppgiftslagen trädde i kraft. I datalagen avsågs med personregister ett register, förteckning eller andra anteckningar som fördes med hjälp av automatisk databehandling och som innehöll personuppgift som kunde hänföras till den som avsågs med uppgiften. Bara den som anmält sig till Datainspektionen och fått licens fick inrätta och föra personregister. För att få registrera känsliga personuppgifter krävdes, utöver licens, ett särskilt tillstånd från Datainspektionen. Ett sådant tillstånd behövdes t.ex. som regel för att inrätta och föra register med uppgifter om att någon misstänktes eller var dömd för brott, omdömen om den registrerade eller personuppgifter som hämtats från något annat register. Om ett personregister hade beslutats av riksdagen eller regeringen, krävdes dock inget tillstånd.

Genom personuppgiftslagen avskaffades det tidigare licens- och tillståndsförfarandet. Utgångspunkten i personuppgiftslagen är att behandling av personuppgifter är tillåten i de fall och på de villkor lagen anger.

Personuppgiftslagen innehåller generella riktlinjer för all behandling av personuppgifter. Begreppet behandling av personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, exempelvis att samla in, söka, bevara och sprida uppgifter. Lagen omfattar i princip endast behandling av personuppgifter som är helt eller delvis automatiserad. Även manuell behandling kan dock omfattas, nämligen om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Enligt personuppgiftslagen ska en personuppgiftsansvarig se till att personuppgifter behandlas bara om det är lagligt. Den personuppgiftsansvarige ska vidare se till *att* personuppgifter behandlas på ett korrekt sätt och i enlighet med god sed, *att* personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål, *att* de inte behandlas för något ändamål som är oförenligt med det för vilket de samlades in, *att* de personuppgifter som behandlas är riktiga och om nödvändigt aktuella, *att* alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen *och att* personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Vidare reglerar personuppgiftslagen, som nämnts, när behandling av uppgifter är tillåten. Detta är i princip fallet när den registrerade har lämnat sitt samtycke eller när behandlingen är nödvändig av olika angivna skäl, bl.a. för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet och för att den personuppgiftsansvarige, eller tredje

man till vilken personuppgifter lämnas ut, ska kunna utföra en arbetsuppgift i samband med myndighetsutövning.

Personuppgiftslagen förbjuder andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Det finns dock ett bemyndigande för regeringen, eller den myndighet som regeringen bestämmer, att meddela föreskrifter om undantag från förbudet. Datainspektionen har meddelat sådana föreskrifter; DIFS 1998:3, jfr 9 § personuppgiftsförordningen (1998:1191).

Den 1 januari 2007 trädde vissa ändringar av personuppgiftslagen i kraft, som innebär att lagen i viss utsträckning utformas enligt en s.k. missbruksmodell (prop. 2005/06:173). Regleringen tar därmed inte sikte på själva hanteringen av personuppgifterna utan på att uppgifterna inte får missbrukas till skada för någons personliga integritet. Behandling av personuppgifter i ostrukturerat material, t.ex. löpande text och enstaka bild- och ljudupptagningar, undantas från de flesta av personuppgiftslagens detaljerade hanteringsregler. Sådan behandling tillåts utan andra restriktioner än att den registrerades personliga integritet inte får kränkas.

Bestämmelserna i personuppgiftslagen redovisas närmare i samband med de förslag som lämnas i avsnitt 6.4.2.

4.3 Den nuvarande polisregisterlagstiftningen

4.3.1 Polisregisterlagstiftningen

Polisdatalagen trädde i kraft den 1 april 1999. Lagen, som gäller utöver personuppgiftslagen, utgör en del av lagstiftningen om polisens register. Vid sidan av polisdatalagen finns det andra författningar som reglerar behandling av personuppgifter inom polisen. Några av dessa är s.k. registerförfattningar och innehåller uteslutande bestämmelser om personuppgiftsbehandling medan andra endast innehåller ett fåtal sådana bestämmelser, t.ex. om visst register. Bestämmelser om personuppgiftsbehandling finns i vapenlagen (1996:67), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:343) om internationellt polisiärt samarbete, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister, efterlysningskungörelsen (1969:293), passförordningen (1979:664), förordningen (1997:902) om register över strafföreläggande och förordningen (1997:903) om register över föreläggande av ordningsbot. De aktuella författningarna behandlas i anslutning till beskrivningarna av registren i *bilaga 6*.

4.3.2 Polisdatalagen

Polisens möjligheter att föra kriminal- och polisregister reglerades tidigare i lagen (1963:197) om allmänt kriminalregister och lagen (1965:94) om polisregister m.m. Utgångspunkten i dessa lagar var att registren skulle föras manuellt. Det rättsliga stödet för att föra vissa datoriserade

register, t.ex. person- och belastningsregistret, fanns i förordningen (1970:517) om rättsväsendets informationssystem (RI-förordningen). Många polisregister fördes med stöd av Datainspektionens tillstånd enligt datalagen.

Polisdatalagen innehåller endast de särbestämmelser som har ansetts nödvändiga för polisens verksamhet. I övrigt gäller personuppgiftslagen eller särskilda lagar, t.ex. lagen om belastningsregister.

Polisdatalagen gäller vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när något sådant inträffat, eller
3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Lagen omfattar således inte all behandling av personuppgifter inom polisen. Uppgiftsbehandling inom den hjälpande och stödjande verksamheten, tillståndsverksamheten och den administrativa verksamheten faller utanför lagens tillämpningsområde. För personuppgiftsbehandling i sådan verksamhet gäller personuppgiftslagen och eventuell särreglering i annan författning. Som exempel kan nämnas att passregistret regleras av personuppgiftslagen och passförordningen (1979:664).

Inom polisen förs även ett flertal register som i och för sig faller inom polisdatalagens tillämpningsområde men som med tillämpning av lagens övergångsbestämmelser fortfarande förs med stöd av den upphävda datalagen och Datainspektionens tillstånd.

Behandling av personuppgifter som sker med stöd av lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem eller lagen om passagerarregister har uttryckligen undantagits från polisdatalagens tillämpningsområde.

Polisdatalagen innehåller allmänna bestämmelser om behandling av personuppgifter i polisiärt arbete och särskilda bestämmelser om behandling i kriminalunderrättelseverksamhet och om vissa register. Det finns två kategorier av allmänna bestämmelser i lagen, dels sådana som gäller för all behandling av personuppgifter (dvs. även sådan behandling som inte är automatiserad), dels sådana som endast gäller automatiserad behandling. Till den förstnämnda kategorin hör bestämmelser som reglerar behandling av känsliga personuppgifter (5 §), utlämnande av uppgifter, bl.a. till statistikmyndighet och utländsk myndighet (6–8 §§) och bestämmelser om rättelse och skadestånd (9 §). Därutöver gäller för automatiserad behandling även allmänna bestämmelser om behandling av uppgifter om kvarstående misstankar (10–12 §§) och om gallring (13 §).

Enligt de särskilda bestämmelserna om kriminalunderrättelseverksamhet får uppgifter i sådan verksamhet endast behandlas inom ramen för en s.k. särskild undersökning eller i kriminalunderrättelseregister (14–21 §§). De register som regleras särskilt i lagen är – utöver kriminalunderrättelseregister – register med uppgifter om DNA-analyser, fingeravtrycks- och signalementsregister samt SÄPO-registret. Registren behandlas närmare i *bilaga 6.*

4.4 Vissa EU-beslut och lagstiftningsförslag

Inom ramen för EU-samarbetet har under de senaste åren förhandlats och antagits flera rambeslut och rådsbeslut som berör behandling av personuppgifter inom polisen. Flertalet av dessa ger ökade möjligheter för brottsbekämpande myndigheter att utbyta uppgifter inom sitt område. Vidare finns det s.k. dataskyddsrambeslutet, som innehåller bestämmelser om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

I lagrådsremissen Preskription för allvarliga brott föreslås en ändring i polisdatalagen.

4.4.1 Dataskyddsrambeslutet

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) reglerar dataskyddet inom angivna områden. Rambeslutet är föranlett av ett antal nya EU-instrument rörande utvidgat polisiärt och rättsligt samarbete avseende gränsöverskridande informationsutbyte.

Dataskyddsrambeslutet förpliktar medlemsstaterna att behandla uppgifter som utbyts mellan staterna inom ramen för det angivna samarbetet på ett sådant sätt att skyddet för enskildas integritet värnas. Det innehåller bestämmelser som avser att förstärka skyddet vid behandling av personuppgifter som överförs. Rambeslutet utgör ett komplement till andra instrument om informationsutbyte inom ramen för polisiärt och straffrättsligt samarbete. Det innehåller bl.a. bestämmelser om allmänna utgångspunkter för behandlingen av personuppgifter och känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. Till stora delar motsvarar innehållet dataskyddsdirektivet, som i svensk rätt har genomförts i personuppgiftslagen. Vidare finns bl.a. särskilda bestämmelser som begränsar möjligheterna att behandla personuppgifter som mottagits från en annan stat.

Regeringen har i propositionen Godkännande av dataskyddsrambeslutet (prop. 2008/09:16) på ett övergripande plan övervägt vilka lagändringar som kan krävas. Riksdagen godkände utkastet till rambeslut (bet. 2008/09:JuU7, rskr. 2008/09:41), som därefter har antagits av rådet. Rambeslutet har ännu inte genomförts i svensk rätt.

4.4.2 Rådsbeslutet om tillgång till informationssystemet för viseringar

Rådets beslut 2004/512/EG om inrättande av Informationssystemet för viseringar (VIS) ledde till att VIS inrättades år 2004 som ett system för utbyte av viseringsuppgifter mellan medlemsstaterna. Samma år presenterade kommissionen ett förslag till förordning om VIS och utbytet av uppgifter mellan medlemsstaterna om viseringar för kortare vistelser (VIS-förordningen). Ett reviderat förslag till VIS-förordning, Europa-

parlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse, har senare antagits. VIS-förordningen kompletteras inom tredje pelaren av rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott.

Enligt rådsbeslutet ska särskilt utsedda brottsbekämpande myndigheter i medlemsstaterna och Europol under vissa förutsättningar ges tillgång till uppgifter ur VIS i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott. Reglerna för hur myndigheterna får använda registret är restriktiva och uppgifter får endast lämnas ut under vissa speciella förutsättningar. Ett grundläggande krav för att en brottsbekämpande myndighet ska få tillgång till uppgifter i VIS är att den lämnar en motiverad, skriftlig eller elektronisk, begäran till en central åtkomstpunkt som ska kontrollera att samtliga villkor för tillgång till VIS är uppfyllda. Vidare krävs bl.a. att sökningarna är nödvändiga för att förebygga, upptäcka eller utreda terroristbrott eller andra grova brott, att sökningarna krävs i ett specifikt ärende och att det finns rimliga skäl att anse att inhämtandet av VIS-uppgifter väsentligen kommer att bidra till att brotten i fråga förebyggs, upptäcks eller utreds.

Regeringen har i propositionen Godkännande av rådets beslut om åtkomst till informationssystemet för viseringar i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (prop. 2007/08:132) på ett övergripande plan övervägt vilka lagändringar som kan bli nödvändiga med anledning av rådsbeslutet. Riksdagen godkände utkastet till rådsbeslut (bet. 2007/08:JuU27, rskr. 2007/08:250), som därefter har antagits av rådet. Rådsbeslutet har ännu inte genomförts i svensk rätt.

4.4.3 Prümrådsbeslutet

Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, (Prümrådsbeslutet), bygger på en konvention kallad Prümkonventionen, som år 2005 ingicks mellan sju av EU:s medlemsstater. Prümrådsbeslutet innehåller bestämmelser som syftar till att fördjupa det gränsöverskridande samarbetet mellan de myndigheter inom EU som ansvarar för att förebygga och utreda brott. I huvudsak ska detta ske genom förenklade former för utbyte av DNA-profiler, fingeravtryck och uppgifter om fordon. Rådsbeslutet aktualiserar inte inrättande av några nya databaser, utan bygger på ett automatiserat utbyte av uppgifter som redan finns lagrade i medlemsstaternas befintliga databaser. I rådsbeslutet regleras också skyldigheten att översända vissa personuppgifter och andra uppgifter till en annan medlemsstat vid större evenemang med gränsöverskridande verkningar. Därutöver finns en fakultativ bestämmelse om översändande av uppgifter till skydd mot terrorism. Bestämmelserna om uppgiftsutbyte kompletteras med utförliga bestämmelser om dataskydd. Dessa bestämmelser måste genomföras innan uppgiftsutbytet får inledas. Utöver bestämmelserna om informa-

tionsutbyte innehåller rådsbeslutet bestämmelser om frivilligt operativt samarbete.

Regeringen har i propositionen Godkännande av Prümrådsbeslutet (prop. 2007/08:83) på ett övergripande plan övervägt vilka lagändringar som kan krävas. Riksdagen godkände utkastet till rådsbeslut (bet. 2007/08:JuU20, rskr. 2007/08:197). Beslutet har därefter antagits av rådet.

En särskild utredare har i departementspromemorian Genomförandet av delar av Prümrådsbeslutet (Ds 2009:8) bl.a. föreslagit ändringar i polisdatalagen och lagen (2000:343) om internationellt polisiärt samarbete. Förslagen omfattar bara de delar av rådsbeslutet som är tvingande. Promemorian har remissbehandlats. Rådsbeslutet har ännu inte genomförts i svensk rätt.

4.4.4 Rambeslutet om utbyte av uppgifter ur kriminalregister

Rambeslutet 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll har främst intresse för domstolar och åklagare men berör även polisens verksamhet. Rambeslutets syfte är att förbättra och underlätta utbytet av uppgifter ur kriminalregister mellan EU:s medlemsstater.

Uppgifter om brottmålsdomar utbyts för närvarande med stöd av 1959 års europeiska konvention om ömsesidig rättslig hjälp i brottmål. Systemet har visat sig ha betydande brister och domstolar meddelar ofta dom enbart med beaktande av tidigare domar som finns i deras nationella register, men utan kunskap om eventuella domar i andra medlemsstaters register. Enligt rambeslutet ska varje medlemsstat som meddelar en dom mot en medborgare i en annan medlemsstat informera medborgarstaten om domen. Medborgarstaten ska därefter lagra informationen. Rambeslutet lägger också grunden för nästa steg i arbetet med att effektivisera informationsutbytet och möjliggöra elektronisk uppgiftsöverföring, som återspeglas i rådets beslut 2009/316/RIF av den 6 april 2009 om inrättande av det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris) i enlighet med artikel 11 i rambeslut 2009/315/RIF. I propositionen Sveriges antagande av rambeslut om utbyte av uppgifter i kriminalregister (prop. 2008/09:18) har regeringen översiktligt redovisat vilka lagstiftningsåtgärder som kan krävas. Riksdagen godkände utkastet till rambeslut (bet. 2008/09:JuU11, rskr. 2008/09:33). Rambeslutet har därefter antagits av rådet, men ännu inte genomförts i svensk rätt.

4.4.5 Rådsbeslutet om inrättande av Europol

Det fördjupade gränsöverskridande polisiära samarbetet och utbytet av information påverkas av utvecklingen av det polisiära samarbetet inom ramen för EU:s gemensamma polisbyrå, Europol. En av Europols viktigaste uppgifter är att samla in och bearbeta information om allvarlig gränsöverskridande brottslighet av visst slag och att förmedla denna information vidare till medlemsstaterna. Europols verksamhet bygger på möjligheten att från medlemsstaterna hämta in och analysera underrättel-

seinformation om viss grov gränsöverskridande brottslighet och sedan återföra resultatet av analyserna till medlemsstaterna. Den svenska polisens utlämnande av uppgifter sker med stöd av 7 § första stycket polisdatalagen.

Europols verksamhet har hittills byggt på Europolkonventionen (prop. 1996/97:164). Rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av europeiska polisbyrån (Europol) ersätter Europolkonventionen och dess ändringsprotokoll. Genom beslutet förändras den rättsliga grunden för Europols verksamhet från ett mellanstatligt samarbete till att Europol blir ett EU-organ. Europol ges bl.a. möjlighet att upprätta och driva nya system för informationsbehandling, t.ex. när det gäller terroristbekämpning. Rådsbeslutet innehåller också vissa nya bestämmelser om dataskydd, t.ex. inrättande av ett oberoende uppgiftsskyddsombud. Regeringen har i propositionen Godkännande av rådets beslut om inrättande av Europeiska polisbyrån (Europol) på ett övergripande plan övervägt vilka lagändringar som kan krävas (prop. 2008/09:14). Riksdagen godkände utkastet till rådsbeslut (bet. 2008/09:JuU6, rskr. 2008/09:63). Beslutet har därefter antagits av rådet.

Regeringen har i propositionen Immunitet och privilegier för Europol (prop. 2009/10:13) lämnat förslag till den lagändring som måste träda i kraft den dag rådsbeslutet ska börja tillämpas, dvs. den 1 januari 2010. Förslaget består i en ändrad hänvisning i bilagan till lagen (1976:661) om immunitet och privilegier i viss fall. Enligt propositionen avser regeringen att i annat sammanhang överväga behovet av ytterligare lagändringar med anledning av Europolsamarbetet.

4.4.6 Rambeslutet om förenklat informations- och underrättelseutbyte

Den tillgänglighetsprincip som är väsentlig i EU:s arbete för att utveckla informationsutbytet är en av grundstenarna i rambeslutet om förenklat informations- och underrättelseutbyte mellan medlemsstaternas brottsbekämpande myndigheter. Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater kom till efter ett svenskt initiativ. Rambeslutet innebär att brottsbekämpande myndigheter i medlemsstaterna redan på underrättelsestadiet, och över myndighetsgränserna, snabbt ska kunna utbyta befintlig information och befintliga underrättelser. Genom rambeslutet åtar sig medlemsstaterna bl.a. dels att på begäran av en annan stat lämna viss information, dels att spontant lämna vissa uppgifter.

Rambeslutet har genomförts i svensk rätt genom förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen, som trädde i kraft den 1 februari 2009. Förordningen, som bygger på förutsättningen att gällande svensk rätt redan medger utlämnande av sådana uppgifter som ska utbytas enligt rambeslutet, innehåller framförallt bestämmelser om förfarandet i samband med uppgiftsutbytet.

4.4.7 Preskription vid allvarliga brott

I en lagrådsremiss den 8 oktober 2009 har regeringen föreslagit att åtalspreskription, påföljdspreskription och absolut preskription ska avskaffas för vissa brott, om dessa har begåtts av vuxna lagöverträdare. De brott som avses är mord, dråp, grovt folkrättsbrott, folkmord samt terroristbrott som begåtts genom mord eller dråp. Även försök till sådana brott, med undantag för grovt folkrättsbrott, ska enligt förslaget undantas från preskription. Vidare har föreslagits att sådana uppgifter i det spårregister som innehåller DNA-profiler som hänför sig till nyssnämnda brottstyper ska gallras senast sjuttio år efter registreringen, i stället för trettio år. Förslaget innebär en ändring i 27 § polisdatalagen. Ändringarna föreslås träda i kraft den 1 juli 2010.

5 Polisens register

Vissa av polisens samlingar av personuppgifter i elektronisk form är register i ordets traditionella bemärkelse, dvs. avgränsade system där uppgifter förs in på ett systematiserat sätt efter vissa kriterier och är sökbara endast med särskilda sökord. Detta gäller i första hand vissa äldre system. Nya system som också kan betraktas som register är bl.a. misstankeregistret och belastningsregistret. Utvecklingen inom polisen går mot att registerformen överges för mer flexibla datasystem.

Den nuvarande registerstrukturen har sin bakgrund i tiden före polisdatalagen, när Datainspektionen gav polisen tillstånd att föra olika enskilda register. Registerstrukturen är således inte ett resultat av en övergripande och konsekvent planering.

Polisens register kan delas in i tre grupper beroende på vilka bestämmelser som styr behandlingen av uppgifter, nämligen

– register som förs med stöd av bestämmelser om särskilda register i polisdatalagen eller annan lagstiftning,

– register som förs med stöd av allmänna bestämmelser i polisdatalagen och personuppgiftslagen, och

– register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av den upphävda datalagen och tillstånd från Datainspektionen.

En uppdelning kan också göras mellan centrala och lokala register. De centrala registren förs av Rikspolisstyrelsen och innehåller uppgifter från hela landet. De lokala registren förs av en polismyndighet och innehåller därmed i princip bara uppgifter från ett polisdistrikt.

De register som regleras särskilt i polisdatalagen är kriminalunderrättelseregister, register med uppgifter om DNA-analyser i brottmål, fingeravtrycks- och signalementsregister samt SÄPO-registret. Kriminalunderrättelseregister kan föras både på lokal och central nivå, medan övriga register som regleras i polisdatalagen är centrala. Det finns även särskilda bestämmelser om register i lagstiftning som gäller vid sidan av polisdatalagen, t.ex. i lagen om belastningsregister och lagen om misstankeregister. Därutöver finns centrala och lokala register som saknar särskild författningsreglering. Registren förs då med stöd av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen eller med stöd av data-

lagen och Datainspektionens tillstånd enligt övergångsbestämmelserna till polisdatalagen. Exempel på centrala register som saknar särskild författningsreglering är det allmänna spaningsregistret, det centrala brottsspaningsregistret samt beslags- och analysregistren. Rationell anmälningsrutin (RAR) och Datoriserad utredningsrutin (DurTvå) är exempel på sådana register på lokal nivå.

Polisen utvecklar fortlöpande nya system för att stödja sin verksamhet. En redovisning av polisens register kan därför aldrig bli fullständig. I *bilaga 6* redovisas vissa befintliga datasystem som har betydelse i detta sammanhang.

6 En ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

6.1 Behovet av en ny lagstiftning

Regeringens bedömning: En reform av bestämmelserna om polisens behandling av personuppgifter är nödvändig.
Regeringens förslag: En ny lag införs som ersätter polisdatalagen.

Utredningens bedömning och förslag överensstämmer med promemorians.

Remissinstanserna har tillstyrkt eller inte haft några invändningar mot att bestämmelserna om polisens behandling av personuppgifter reformeras genom införandet av en ny lag som ersätter polisdatalagen.

Promemorians bedömning och förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser delar promemorians bedömning eller har inget att invända mot den. Flertalet remissinstanser tillstyrker eller har inget att invända mot promemorians förslag. Invändningar framförs dock mot enskildheter i förslaget. Även mer generella synpunkter framförs.

Rikspolisstyrelsen uppskattar ambitionen att utöka polisens möjligheter att behandla personuppgifter i bl.a. underrättelseverksamhet. Den föreslagna lagen kommer enligt styrelsen att underlätta informationsutbytet såväl inom polisen som mellan polisen och andra myndigheter. Styrelsen anser dock att det vore olyckligt om en ny lagstiftning i syfte att skydda den personliga integriteten utformas som en hanteringslagstiftning som i detalj reglerar polisens arbetsmetoder. Rikspolisstyrelsen anser att vissa av bestämmelserna, bl.a. de föreslagna sökbegränsningarna, utgör just en sådan detaljreglering som styrelsen är emot. *Säkerhetspolisen* framhåller att det är nödvändigt att arbetet inriktas mot en gemensam lagstiftningsteknik för behandlingen av personuppgifter inom den brottsbekämpande verksamheten och anser att de förslag som läggs fram i promemorian för att komma till rätta med problemen med den alltmer föråldrade polisdatalagen är lovvärda.

Kammarrätten i Stockholm instämmer i att lagstiftning som reglerar användningen av datorstöd måste vara teknikoberoende och flexibel

samtidigt som hänsyn till enskildas integritet tas. Kammarrätten anser att de avvägningar som görs mellan effektiviteten i brottsbekämpningen och skyddet för den personliga integriteten är väl redovisade och motiverade men framhåller, liksom några andra remissinstanser, att det är svårt att förutse förslagets sammantagna konsekvenser. Kammarrätten betonar därför, liksom flera andra remissinstanser, bl.a. *Domstolsverket*, vikten av att lagstiftningen noga utvärderas. *Åklagarmyndigheten* anser att det är uppenbart och glädjande att förslagen och övervägandena i promemorian bygger på ambitionen att reglerna om polisens personuppgiftsbehandling ska stödja modern brottsbekämpning. Åklagarmyndigheten är dock bekymrad över att såväl den gällande som den föreslagna regleringen är mycket svårtillgänglig. *Ekobrottsmyndigheten* anser att det är tveksamt om den föreslagna lagen innebär ett så tydligt klargörande av polisens möjligheter att behandla personuppgifter som behövs för en effektiv men också rättssäker brottsbekämpning. *Kriminalvården* anser att den föreslagna lagen är omfattande och detaljerad. Enligt Kriminalvården bör det övervägas om det inte är tillräckligt att endast ramarna för när behandling av personuppgifter är tillåten och de från integritetsskyddssynpunkt viktigaste bestämmelserna framgår av lagen. Kriminalvården menar att lagen kan kompletteras av mer detaljerade bestämmelser i författningar på lägre nivå med närmare avvägningar av integritetsskyddet.

Datainspektionen avstyrker att promemorians förslag läggs till grund för lagstiftning och föreslår att en kommitté tillsätts med uppdrag att utifrån polisens verksamhet och behov utarbeta ett lagförslag som förmår tillgodose skyddet för den personliga integriteten. Inspektionen anser att den analys som ligger till grund för lagförslaget är bristfällig. *Sveriges advokatsamfund* anser att den föreslagna regleringen har utformats så att verkningarna från integritetsskyddssynpunkt blir synnerligen svåra att överblicka och att dessa behöver genomlysas ytterligare innan en ny reglering införs. Advokatsamfundet förordar ett mer samlat grepp för att komma till rätta med både det alltför stora antalet skilda lagar om myndigheters personuppgifts- och registerhantering och den bristande överensstämmelsen mellan grundläggande begrepp i dessa lagar. *Justitiekanslern* anser att det är svårt att bedöma förslaget på grund av brister i redovisningen av avvägningen mellan verksamhetsbehov och integritetsintressen. Justitiekanslern anser sig därför inte med tillräcklig grad av säkerhet kunna ställa sig bakom de enskilda förslagen i promemorian. Samtidigt anser sig Justitiekanslern inte ha tillräcklig grund för att rikta konkreta invändningar mot förslagen annat än vad gäller vissa gallringsfrister och personuppgiftsbehandling vid vissa yttrandefrihets- och tryckfrihetsbrott.

Skälen för regeringens bedömning och förslag

Allmänt om reformbehovet

Information är en av polisens viktigaste resurser för att uppnå statsmakternas mål i det brottsbekämpande arbetet. Sedan många år är modern informationsteknik en naturlig del i polisens arbete och numera utförs praktiskt taget allt polisarbete mer eller mindre med hjälp av sådan teknik. En väl utnyttjad informationsteknik är därför av stor betydelse för

polisens möjligheter att bedriva sin verksamhet på ett effektivt och rättssäkert sätt. Samtidigt måste informationshanteringen ske med respekt för enskildas integritet.

Som både Polisdatautredningen och promemorian framhåller uppfyller dagens lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet inte de krav som polisens verksamhet ställer på automatiserad behandling av uppgifter. Det finns även brister vad gäller skyddet för den personliga integriteten. En reform är därför nödvändig. Även remissinstanserna instämmer i behovet av reformering av gällande lagstiftning.

Polisdatalagen reglerar bara delar av personuppgiftsbehandlingen

En svaghet i den nuvarande regleringen är bl.a. att den bara täcker delar av personuppgiftsbehandlingen i den brottsbekämpande verksamheten. När polisdatalagen trädde i kraft den 1 april 1999 fördes ett stort antal av polisens register med stöd av Datainspektionens tillstånd enligt den numera upphävda datalagen. För att få möjlighet att anpassa dessa register till den nya lagstiftningen tilläts polisen under en begränsad tid att fortsätta att föra dem med stöd av de äldre bestämmelserna. Flera av registren har dock inte anpassats till polisdatalagen och bedömningen har gjorts att de inte kan föras med stöd av den lagen utan anpassning. Övergångsbestämmelserna till polisdatalagen har därför successivt förlängts för att möjliggöra fortsatt behandling i registren. I propositionen Övergångsbestämmelserna till polisdatalagen (prop. 2009/10:23) föreslås ytterligare förlängning till utgången av juni 2012.

Ett flertal av polisens register förs således fortfarande med stöd av den upphävda datalagen och Datainspektionens tillstånd. Som *Datainspektionen* framhåller innebär detta att polisens personuppgiftsbehandling styrs av två parallella regleringar, vilket skapar såväl tillämpningsproblem som en svåröverskådlig registerstruktur hos polisen. Det behövs därför en ny reglering som ersätter de nuvarande parallella systemen.

Behovet av en teknikneutral lagstiftning

Polisen lagrar personuppgifter i ett stort antal olika databaser. Samma personuppgift kan lagras på flera olika ställen, i olika register och ärendehanteringssystem. Rikspolisstyrelsen gör bedömningen att detta sätt att hantera uppgifter kan leda till kvalitetsbrister, vilket påtalas av styrelsen i en skrivelse till Justitiedepartementet (dnr Ju2007/478/PO). Rikspolisstyrelsen framhåller där att den nuvarande lagstiftningen bl.a. resulterat i en dubbel eller flerdubbel lagring av identiska personuppgifter. Samma eller i det närmaste samma uppgifter lagras i flera system eller register där syftet med behandlingen till vissa delar kan skilja sig åt. Detta för med sig att det uppstår en inkonsistens i informationen. Enligt Rikspolisstyrelsen är det i princip omöjligt för en informationsägare eller enskild handläggare att känna till alla de system där information om en person finns lagrad för att bl.a. genomföra rättningar och gallringar. I huvudsak samma uppgifter i olika register görs tillgängliga för den användare som getts behörighet till registren. Rikspolisstyrelsen påtalar att detta förhål-

lande sammantaget med dubbellagring i ett stort antal register innebär att många enskilda handläggare har eller kan få tillgång till ett stort antal register och därmed också tillgång till mer information än vad som ursprungligen varit avsett. Detta försvårar också möjligheterna att kunna utreda vilken information en tjänsteman har eller har haft tillgång till. Rikspolisstyrelsen konstaterar att lagstiftarens ambition att med de metoder som valts skapa begränsningar för att skydda den enskildes integritet kan te sig fullgott men fungerar i praktiken mindre bra såväl för användaren som till skydd för integriteten. Styrelsen planerar en modernisering av polisens datasystem. Tanken är att de uppgifter som behandlas i polisens verksamhet ska lagras gemensamt på en plats i stället för i separata register. Uppgifterna ska alltså i princip inte registreras och lagras mer än en gång. Tillgången till uppgifterna ska i de allra flesta fall inte – såsom i polisens nuvarande system – vara beroende av att en uppgift finns i ett särskilt register utan vara avhängigt andra kriterier, hänförliga till uppgifterna som sådana och till användarens behörighet. Enligt Rikspolisstyrelsen kommer det planerade datasystemet att möjliggöra ett bättre integritetsskydd. Det blir bl.a. lättare att bygga upp behörighetssystem som gör det möjligt att enklare avgränsa en enskild tjänstemans tillgång till de uppgifter som han eller hon behöver för att kunna utföra sina arbetsuppgifter. Tjänstemannens behov av information kan därigenom tillgodoses på ett rättssäkert sätt. En annan fördel är att det blir enklare att hålla lagrad information uppdaterad och tillförlitlig, eftersom utgångspunkten är att varje uppgift ska lagras endast en eller ett fåtal gånger. Risken att uppgifter bevaras i systemet längre än nödvändigt minskar också. Enligt Rikspolisstyrelsen kommer det över huvud taget att bli lättare att med det nya systemet avgränsa, kontrollera och övervaka all elektronisk tillgång till uppgifter.

Rikspolisstyrelsens arbete med att förändra polisens datasystem har redan inletts. För att styrelsen ska kunna fullfölja det arbetet krävs det en mera teknikneutral lagstiftning som är mindre knuten till registerbegreppet än vad som är fallet med polisdatalagen. Med en mera teknikneutral lagstiftning överlåts i större utsträckning till polisen att avgöra hur insamlade uppgifter ska struktureras och göras åtkomliga i verksamheten.

Utvecklingen går generellt mot att behandling av personuppgifter i traditionella register överges. Både registerbegreppet och begreppet databas har kritiserats i tidigare lagstiftningsärenden. Som exempel kan nämnas propositionen om Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling (prop. 2004/05:164 s. 60 f.). Skälen för detta är bl.a. att begreppen leder tanken till ett visst, i tekniskt avseende avgränsat, informationssystem där informationen har strukturerats på ett visst sätt. Behandling av personuppgifter kommer i framtiden i större utsträckning att ske i avancerade ärendehanteringssystem som länkas samman med varandra, ibland med digital dokumenthantering. I sådana system kan information struktureras på ett sådant sätt att systemet utöver att tjäna som ett verksamhetsstöd för ärendehanteringen även i praktiken tillgodoser samma behov som traditionella personregister genom att olika sökingångar skapas. Det huvudsakliga syftet med insamlingen av personuppgifter är i dessa fall utförandet av en viss arbetsuppgift, inte att registrera uppgifterna i ett personregister.

Det finns uppenbara nackdelar med att som nu behandla personuppgifter inom polisen i ett stort antal separata register. I en sådan struktur är det svårt att hålla alla uppgifter korrekta och uppdaterade. Det är vidare otidsenligt och resurskrävande att registrera samma uppgift flera gånger och att förvalta och administrera ett flertal olika system. Som Rikspolisstyrelsen framhåller är det mera ändamålsenligt att skapa ett system där utgångspunkten är att varje uppgift lagras endast på ett ställe och därifrån görs tillgänglig för olika berättigade ändamål. Uppgifter lagras då i större utsträckning i det sammanhang som de lagligen samlades in. Därmed blir det lättare att hålla en uppgift korrekt och uppdaterad samtidigt som det blir tydligare för den som får åtkomst till uppgiften varför uppgiften har samlats in och behandlas inom polisen.

Utgångspunkten bör således vara att skapa en så teknikneutral och flexibel lagstiftning som möjligt för polisens behandling av personuppgifter i den brottsbekämpande verksamheten. Ingen remissinstans har ifrågasatt denna utgångspunkt. Med en sådan lagstiftning skapas också möjligheter att komma till rätta med de av Rikspolisstyrelsen påtalade problemen beträffande bl.a. dubbellagring, tillgång till information, rättelse och gallring som dagens regelverk för med sig.

Den nya lagen bör således ge ramarna för polisens personuppgiftsbehandling utan att närmare reglera formerna för behandlingen. Detta innebär dock inte att polisen själv ska få avgöra *vilken* personuppgiftsbehandling som ska vara tillåten. En mer teknikneutral lagstiftning förutsätter att det – i syfte att värna den personliga integriteten – införs bestämmelser som reglerar polisens möjlighet att behandla personuppgifter. Vidare måste det ställas höga krav på kontroll och tillsyn av verksamheten, både internt och externt.

Bättre förutsättningar för brottsförebyggande arbete och informationsutbyte

Ett effektivt brottsbekämpande arbete förutsätter att de brottsbekämpande myndigheterna har goda möjligheter att samla in och bearbeta information av olika slag. De uppgifter som behöver kunna samlas in och bearbetas är såväl uppgifter med anknytning till konkreta brott (dvs. uppgifter i brottsutredningar) som uppgifter som avser förväntad eller pågående brottslig verksamhet (dvs. uppgifter i kriminalunderrättelseverksamhet). Förutsättningarna för ett effektivt brottsbekämpande arbete har inte i alla avseenden beaktats vid utformningen av polisdatalagen, vilket lett till vissa tillämpningsproblem.

Ett exempel är oklarheterna kring begreppet kriminalunderrättelseverksamhet. Enligt den nuvarande lagstiftningen får uppgifter i sådan verksamhet behandlas endast under vissa förutsättningar. Behandling får ske

– om en särskild undersökning har inletts under ledning av Rikspolisstyrelsen eller en polismyndighet och det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas, eller

– inom ramen för registrering i kriminalunderrättelseregister.

Det har ifrågasatts om inte behandlingen av personuppgifter i vissa faktiskt existerande polisregister till viss del utgör kriminalunderrättelseverksamhet i polisdatalagens mening. Behandlingen skulle därmed vara

tillåten bara inom ramen för en särskild undersökning eller i kriminalunderrättelseregister. Det är vidare osäkert i vilken utsträckning behandling av underrättelseuppgifter får ske lokalt, dvs. av en enskild tjänsteman genom användning av ordbehandling och e-post m.m. samt genom digital bild- och ljudupptagning. Det finns alltså behov av en reglering som undanröjer dessa och andra oklarheter.

Utvecklingen av polisverksamheten förutsätter, vilket *Rikspolisstyrelsen* poängterar, att polisen i större utsträckning tillåts att behandla personuppgifter för brottsförebyggande ändamål. Sådan behandling sker främst inom ramen för kriminalunderrättelseverksamhet. Enligt äldre synsätt skulle polisens brottsbekämpande verksamhet väsentligen vara reaktivt inriktad. Utgångspunkten var att polisen skulle ägna sig åt att utreda misstankar om konkreta brott och att personer som inte var misstänkta för konkreta brott skulle lämnas i fred. Denna utgångspunkt har övergetts och polisen arbetar sedan länge även proaktivt. Detta arbetssätt förutsätter behandling av uppgifter om misstankar mot enskilda personer redan vid en låg grad av misstanke och även om misstanken inte kunnat preciseras till att avse en viss specifik händelse eller gärning. Polisen har utvecklat en modell för ledning och styrning av verksamheten där polisens kriminalunderrättelseverksamhet spelar en avgörande roll, polisens underrättelsemodell (PUM). Modellen innebär att de polisiära underrättelser och de analyser som kriminalunderrättelseverksamheten tar fram ska ligga till grund för ledningens prioriteringar och inriktning av den operativa verksamheten. Kunskapen används för att polisen på alla nivåer ska kunna göra riktiga prioriteringar och använda adekvata operativa metoder och resurser för olika typer av problem. Som Polisdatautredningen konstaterar ligger det i sakens natur att en brottsförebyggande arbetsmetod innebär en ökad risk för intrång i den enskildes personliga integritet jämfört med ett reaktivt arbetssätt, men att detta måste vägas mot effektiviteten i brottsbekämpningen (SOU 2001:92 s. 113). Regeringen delar denna uppfattning och anser vid en samlad bedömning att polisen bör ges ökat utrymme att behandla information i sitt brottsförebyggande arbete.

Polisen bör generellt ges bättre möjligheter att utnyttja den information och kunskap som finns inom den samlade organisationen. Flera av polisens nuvarande register förs lokalt vid respektive polismyndighet och åtkomsten till registren begränsas i regel till tjänstemän vid den egna myndigheten. Som exempel kan nämnas att polisen i princip endast har tillgång till de brottsanmälningar som gjorts i det egna polisdistriktet, eftersom varje polismyndighet har sitt eget register över brottsanmälningar (Rationell anmälningsrutin; RAR). På samma sätt förekommer det att olika organisatoriska enheter inom en myndighet inte har tillgång till insamlad information på ett effektivt och ändamålsenligt sätt. Sammantaget bör enligt regeringens mening polisen ges bättre möjligheter att ta till vara och tillgängliggöra den samlade informationen inom polisen. Utgångspunkten bör vara att behovet av information ska styra tillgången till uppgifterna. Tillgången ska inte vara beroende av var informationen har samlats in eller lagrats.

Bättre förutsättningar för att samverka i brottsbekämpningen

Från brottsbekämpningssynpunkt är det angeläget att samhällets samlade resurser används rationellt och effektivt. En väl utvecklad samverkan mellan de brottsbekämpande myndigheterna ger bättre förutsättningar att förhindra och klara upp brott, inte minst grova brott. Detta framhålls bl.a. i departementspromemorian Nationell mobilisering mot den grova organiserade brottsligheten – överväganden och förslag (Ds 2008:38), i vilken lämnas förslag på åtgärder som syftar till att lägga grunden till en effektivare och mer uthållig bekämpning av den grova organiserade brottsligheten.

En utgångspunkt för den nya lagstiftningen måste vara att, med beaktande av befogade krav på skydd för enskildas integritet, var och en av de brottsbekämpande myndigheterna kan få tillgång till uppgifter från andra brottsbekämpande myndigheter, i den mån uppgifterna behövs i verksamheten.

Ett stort antal av remissinstanserna har välkomnat promemorians tydliga målsättning att möjliggöra ett utökat och mer effektivt informationsutbyte mellan de brottsbekämpande myndigheterna.

Den grova brottsligheten är också ofta gränsöverskridande. Det internationella polisiära samarbetet är därför av stor betydelse för möjligheten att bekämpa sådan brottslighet. Sverige har i olika internationella överenskommelser förbundit sig att bistå andra länder med brottsbekämpande åtgärder av skilda slag. En ny reglering av polisens behandling av personuppgifter i den brottsbekämpande verksamheten bör därför ge polisen goda möjligheter att utbyta information inom ramen för det internationella samarbetet.

En utvecklad samverkan är också utgångspunkten för det arbete som sedan mitten av 1990-talet bedrivs av Rådet för rättsväsendets informationsförsörjning (RIF). Arbetet syftar bl.a. till en gemensam säkerhets- och kommunikationslösning mellan myndigheterna i rådet.

Bör promemorians förslag ligga till grund för lagstiftning eller krävs det ytterligare överväganden?

Några remissinstanser kritiserar promemorians förslag. *Datainspektionen, Sveriges advokatsamfund* och *Justitiekanslern* anser bl.a. att promemorian brister i redovisningen av avvägningen mellan verksamhetsintressen och integritetsskyddsintressen. Både *Datainspektionen* och *Sveriges advokatsamfund* förordar att frågorna utreds ytterligare. Några remissinstanser som i och för sig ställer sig bakom förslaget i stort, bl.a. *Kammarrätten i Stockholm* och *Säkerhetspolisen,* pekar på att det är svårt att överblicka de sammantagna konsekvenserna av förslaget. Andra remissinstanser, bl.a. *Rikspolisstyrelsen* och *Åklagarmyndigheten*, anser att promemorians lagförslag är för detaljerat och svårtillgängligt och att det i alltför stor utsträckning begränsar polisens möjlighet att behandla personuppgifter.

Det finns flera skäl till att det är komplicerat att utforma lagstiftning som reglerar behandlingen av personuppgifter i polisens brottsbekämpande verksamhet. Polisens verksamhet består av en mängd disparata uppgifter. Polisen hanterar också i stor utsträckning integritetskänslig

information. Det är svårt att hitta en optimal balans mellan verksamhetsintressen och integritetsskyddsintressen. Det är därför inte förvånande att de brottsbekämpande myndigheterna å ena sidan och de myndigheter som har till huvuduppgift att värna den personliga integriteten å den andra har framfört diametralt olika kritiska synpunkter mot förslaget.

I och med att i stort sett all informationshantering inom polisen sker med stöd av datorer och att informationen i stor utsträckning innehåller personuppgifter är det ofrånkomligt att en personuppgiftslag påverkar polisens arbetssätt. En alltför detaljerad och begränsande reglering skulle enligt regeringens mening kunna försämra polisens förutsättningar att bekämpa brott. Från integritetsskyddssynpunkt är det dock uteslutet att helt överlåta åt polisen att utifrån verksamhetsintressen själv avgöra vilken behandling av personuppgifter som bör få ske.

En annan omständighet som gör lagstiftningsarbetet på området komplicerat är den ständigt pågående tekniska utvecklingen. Nya möjligheter att hantera information skapas fortlöpande vilket medför att bl.a. begreppsbildning snabbt blir inaktuell. Äldre lagstiftning och i viss mån även dataskyddsprinciper utgår t.ex. i stor utsträckning från att personuppgifter lagras och struktureras i särskilda register för särskilt angivna ändamål. Moderna system skapas inte på detta sätt. Utvecklingen går t.ex. mot att hela aktmaterial behandlas digitalt. En ny lagstiftning på området måste förhålla sig till att det numera finns tekniska möjligheter att lagra mycket stora mängder uppgifter under i stort sett obegränsad tid, att uppgifterna kan göras tillgängliga genom avancerade sökmotorer och att olika uppgiftssamlingar kan länkas samman på ett otal olika sätt, att uppgifterna kan göras tillgängliga via olika former av mobil utrustning, att insamling och överföring av ljud och bild kan ske digitalt och att uppgifter kan bearbetas i avancerade analyssystem. Det ligger i sakens natur att det inte i detalj går att lagreglera hur polisen och andra myndigheter ska få hantera information digitalt. Utgångspunkten måste i stället vara att skapa generella bestämmelser till skydd för den personliga integriteten.

Frågan är då om det behövs ytterligare beredningsunderlag i detta lagstiftningsärende, vilket bl.a. *Datainspektionen* anser. Som underlag för arbetet finns dels Polisdatautredningens betänkande, dels en departementspromemoria som tagits fram inom Justitiedepartementet. Såväl betänkandet som promemorian har remissbehandlats. Vid utarbetandet av departementspromemorian har man övervägt det som framkommit i remissvaren på Polisdatautredningens betänkande. Likaså har betänkanden och lagstiftning på angränsande områden studerats, t.ex. beträffande Tullverket, Försvarsmakten och Kustbevakningen. Ett flertal bestämmelser i promemorians lagförslag svarar mot bestämmelser i motsvarande reglering för dessa myndigheter och förslagets struktur liknar i flera avseenden bl.a. Tullverkets lagstiftning om behandling av uppgifter i dess brottsbekämpande verksamhet. Det beredningsunderlag som nu finns motsvarar väl det krav som bör ställas på underlaget i ett lagstiftningsprojekt av detta slag. Det saknas därför skäl att inhämta ytterligare beredningsunderlag. Det kan dock finnas skäl att i annat sammanhang försöka uppnå större enhetlighet i begreppsbildningen på registerlagstiftningens område, vilket *Sveriges advokatsamfund* förordar.

Flera remissinstanser framför uppfattningen att det är svårt att fullt ut överblicka de sammantagna konsekvenserna av en ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Att ställa ett sådant krav på en lagstiftning av detta slag låter sig dock svårligen göras. Komplex lagstiftning måste kunna beslutas och genomföras utan att varje enskildhet kan förutses. Det är emellertid viktigt att lagstiftningen utvärderas, vilket diskuteras i avsnitt 17.3.

Den kritik som framställs av remissinstanserna, både den mer övergripande och den som rör enskildheter i förslaget, kommer att beröras i de följande avsnitten.

En ny lag om behandling av personuppgifter inom polisen

Personuppgiftslagen gäller generellt för all behandling av personuppgifter, såvida det inte finns en särskild registerförfattning för viss behandling. I det lagstiftningsärende som föregick personuppgiftslagen uttalade regeringen att lagen i princip bara bör innehålla generella regler och att behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar (prop. 1997/98:44 s. 40 f.). Sådan författningsreglering, genom s.k. registerlagar, har skett utifrån det principiella ställningstagandet att myndighetsregister med ett stort antal registrerade personer och ett integritetskänsligt innehåll bör regleras i lag. Registerförfattningar finns för ett flertal olika myndigheters verksamheter, bl.a. för övriga myndigheter med brottsbekämpande uppgifter. För polisens del utgör bl.a. polisdatalagen en sådan lag.

Det finns inget skäl att nu göra någon annan bedömning när det gäller behovet av en särlagstiftning för polisens behandling av personuppgifter i den brottsbekämpande verksamheten. Det bör alltså även i fortsättningen finnas en särskild lag för sådan behandling av personuppgifter. För att bättre tillgodose kravet på en effektiv brottsbekämpande verksamhet som också väl tillgodoser den personliga integriteten bör polisdatalagen ersättas med en ny lag.

6.2 Lagens syfte och skyddet för den personliga integriteten

Regeringens förslag: Syftet med lagen ska vara att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter i polisens brottsbekämpande verksamhet och att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sådan verksamhet.

Utredningens förslag överensstämmer med promemorians.

Remissinstanserna har inte yttrat sig särskilt i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår dock en annan utformning av bestämmelsen om lagens syfte.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag och bedömning. Några remissinstanser, däribland *Kammarrätten i Stockholm*, *Ekobrottsmyndigheten* och *Rikspolisstyrelsen*, anser dock att det i författningstexten uttryckligen bör anges att lagen, utöver att skydda den personliga integriteten, också syftar till att främja en effektiv brottsbekämpning.

Skälen för regeringens förslag: En effektiv och rättssäker brottsbekämpning förutsätter att polisen har ett bra verksamhetsstöd i form av en väl fungerande informationsteknik. Polisen måste i olika typer av utredningar och undersökningar ha möjlighet att samla in, registrera, behandla och lagra uppgifter av vitt skilda slag, bl.a. om misstänkta, målsägande, vittnen och andra personer. Uppgifter måste också vid behov kunna tillhandahållas elektroniskt till ett större antal personer vid en eller flera polismyndigheter eller andra brottsbekämpande myndigheter. Åklagare som leder förundersökningar kan t.ex. ha behov av att elektroniskt få tillgång till uppgifter från polisen. Uppgifter måste också – inom ramen för det internationella samarbetet – kunna utbytas elektroniskt med brottsbekämpande myndigheter i andra länder.

Hantering av personuppgifter på det nu beskrivna sättet kan innebära en risk för intrång i den personliga integriteten. Det är viktigt att hitta en väl avvägd balans mellan å ena sidan skyddet för den personliga integriteten och å andra sidan samhällets rättmätiga krav på att brott förebyggs och förhindras samt att brott utreds och personer som begår brott lagförs. Att brott utreds och att misstänkta lagförs är ett uttryck för att statsmakterna menar allvar med straffbuden och beaktar brottsoffrens intresse. Intrång i den personliga integriteten måste dock alltid stå i rimlig proportion till det intresse som ska tillgodoses med behandlingen av personuppgifterna.

De grundläggande bestämmelserna till skydd för den personliga integriteten finns i regeringsformen och det är i första hand personuppgiftslagen som ska tillgodose regeringsformens krav i fråga om integritetsskydd i automatiserad personuppgiftsbehandling, se avsnitt 4.1. Personuppgiftslagen kompletteras, såvitt nu är av intresse, av polisdatalagen. Integritetsskyddande bestämmelser om utlämnande av personuppgifter finns även i övriga registerlagar som reglerar polisens register, liksom i offentlighets- och sekretesslagen.

Begreppet personlig integritet är inte definierat vare sig i lag eller annan författning. Ett sätt att beskriva begreppet är dock att skilja mellan olika former av handlanden som kan anses kränka den personliga integriteten. Man kan då sortera in handlanden som utgör intrång i integriteten i tre huvudkategorier: 1) intrång i en persons privata sfär, oavsett om det sker i fysisk eller annan mening; 2) insamlande av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annan användning av uppgifter om en persons privata förhållanden (se Stig Strömholm, SvJT 1971 s. 695 och Individens skyddade personlighetssfär i Om våra rättigheter. Antologi utgiven av Rättsfonden, 1980, samt Integritetsskyddskommitténs delbetänkande Skyddet för den personliga integriteten. Kartläggning och analys. Del 1 [SOU 2007:22] s. 52 f.). Ett annat sätt att beskriva begreppet är att skilja mellan olika former av integritet med utgångspunkt från bl.a. de grundläggande fri- och rättigheterna i 2 kap. regeringsformen (se t.ex. SOU 1984:54 s. 42). Med denna utgångspunkt

utgör regler om dataskydd bestämmelser som tar sikte på den personliga integriteten när det gäller respekten för privatlivet. Bestämmelser om skydd för privatlivet kan också sägas vara inriktade på att tillvarata integriteten i ideell mening (se SOU 1992:84 s. 187). Gemensamt för beskrivningarna synes vara att de alla utgår från att en kränkning av integriteten innebär ett oönskat intrång i en fredad sfär som den enskilde bör vara tillförsäkrad (prop. 2005/06:173 s. 15).

Även om det alltså inte är möjligt att entydigt definiera vad som avses med begreppet personlig integritet torde det stå klart att vissa faktorer är särskilt viktiga att ta hänsyn till när det gäller att bedöma intrånget i den personliga integriteten vid automatiserad behandling av personuppgifter. Sådana faktorer är arten av de personuppgifter som ska få behandlas, vilka som ska ha tillgång till uppgifterna – genom direktåtkomst eller på annat sätt –, hur sökning ska få ske, hur lång tid personuppgifterna ska få sparas samt vilken kontroll av verksamheten som finns. Ju fler uppgifter som får behandlas, ju större möjligheter till sammanställningar och sökningar som ges och ju längre tid som uppgifterna får sparas, desto större är, typiskt sett, risken för integritetsintrång. Ju större risken för intrång är, desto mer angeläget måste ändamålet med personuppgiftsbehandlingen vara.

I 2 kap. 12 § andra stycket regeringsformen finns en proportionalitetsprincip som innebär att viss rättighetsinskränkande lagstiftning aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Även om bestämmelsen inte gäller för 2 kap. 3 § andra stycket regeringsformen, som reglerar integritetsskyddet vid automatisk behandling av personuppgifter, anses det att en proportionalitetsprincip i vid mening gäller för all lagstiftning som inskränker de grundläggande fri- och rättigheterna. En proportionalitetsprincip finns också i Europakonventionens artikel 8, som reglerar rätten till skydd för privat- och familjeliv.

Mot bakgrund av det ovan sagda måste den närmare utformningen av de nya bestämmelserna om behandling av personuppgifter i polisens brottsbekämpande verksamhet föregås av en avvägning mellan å ena sidan intresset av en effektiv brottsbekämpning och å andra sidan intresset av skydd för den personliga integriteten. Vid den avvägningen finns det anledning att hålla i minnet att de uppgifter som kan bli aktuella att behandla ofta är särskilt integritetskänsliga, dels därför att de kan peka ut personer såsom misstänkta för brott, dels därför att de inte sällan rör enskildas personliga sfär. Blotta det förhållandet att omfattande uppgifter om en enskilds privata förhållanden kan komma att sammanställas och göras tillgängliga inom polisens verksamhet kan uppfattas som ett integritetsintrång.

I de följande avsnitten diskuteras ingående hur polisens behov av att kunna behandla vissa uppgifter lämpligen bör vägas mot behovet av skydd för den personliga integriteten. I dessa avsnitt behandlas också den kritik som bl.a. *Datainspektionen* framför mot promemorians förslag när det gäller skyddet för den personliga integriteten. Det finns dock skäl att redan här redovisa några allmänna utgångspunkter för övervägandena.

Det är till att börja med viktigt att den nya lagen tydligt anger för vilka ändamål behandling av personuppgifter ska få ske. Vidare bör det, på samma sätt som nu, finnas särskilda bestämmelser som begränsar möj-

ligheterna att behandla s.k. känsliga personuppgifter, dvs. uppgifter om någons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Risken för otillbörliga intrång i den personliga integriteten är självfallet större när uppgifter registreras och lagras på ett sådant sätt att flera personer vid en eller flera myndigheter har möjlighet att ta del av dem, än när en enskild tjänsteman behandlar uppgifter vid sin egen dator utan att någon annan har åtkomst till uppgifterna. Det bör därför i lagen införas mera inskränkande bestämmelser för sådan behandling av personuppgifter som innebär att uppgifterna görs åtkomliga för en större krets – görs gemensamt tillgängliga – i den brottsbekämpande verksamheten än för behandling av personuppgifter som inte har gjorts gemensamt tillgängliga.

En förutsättning för att polisen ska kunna bedriva ett effektivt brottsförebyggande arbete är att polisen får behandla uppgifter om personer som inte är misstänkta för något konkret brott, men ändå misstänks ägna sig åt brottslig verksamhet. Att ge polisen möjlighet att bygga upp samlingar av uppgifter om enskilda, utan att det finns någon anknytning till ett visst brott, kan emellertid inge betänkligheter från integritetssynpunkt. En utgångspunkt bör därför vara att det bör gälla större restriktivitet för behandlingen av uppgifter som inte har samband med ett konkret brott än för behandlingen av uppgifter som behövs för att utreda och beivra ett visst brott.

I ett integritetsskyddsperspektiv är det också viktigt att särskilja olika typer av uppgifter. Det är särskilt viktigt att det inte uppstår oklarheter om huruvida den person som en behandlad uppgift rör är misstänkt eller inte. Detta kommer bl.a. till uttryck i Europarådets rekommendation No. R (87) 15 om användningen av personuppgifter inom polissektorn (se avsnitt 4.2.3). En utgångspunkt för den nya lagstiftningen bör vara att det ska framgå huruvida behandlingen sker för att personen är misstänkt eller inte. Likaså bör tillförlitligheten av behandlade uppgifter kunna utläsas, exempelvis om informationen består av kontrollerade fakta eller av endast antaganden eller obekräftade påståenden.

När det bedöms vilket intrång i den personliga integriteten som olika former av behandling av personuppgifter innefattar, finns det anledning att särskilt beakta i vilken utsträckning uppgifterna kan användas för sökning och sammanställning. Ju större möjligheter det finns att söka och sammanställa insamlade och lagrade uppgifter, desto större är risken för att behandlingen av personuppgifter leder till intrång i de registrerades personliga integritet. Mot denna bakgrund bör utgångspunkten vara att reglerna utformas så att endast en viss, begränsad information, erhålls initialt när namn eller personnummer eller andra liknande identitetsbeteckningar, som kan hänföras till en bestämd individ, används som sökbegrepp i polisens brottsbekämpande verksamhet.

Som redan nämnts måste de brottsbekämpande myndigheterna kunna utbyta information sinsemellan och, i viss utsträckning, lämna information till andra myndigheter. För att kunna utbyta uppgifter på ett effektivt och rättssäkert sätt behöver myndigheterna kunna utnyttja tillgängliga tekniska hjälpmedel. Av särskild betydelse är möjligheten att vid behov snabbt kunna få tillgång till uppgifter hos andra myndigheter på automatiserad väg, exempelvis genom direktåtkomst. En sådan möjlighet kan

dock innebära ökade risker för integritetsintrång. Det beror framförallt på att system för direktåtkomst torde innebära att antalet personer som har tillgång till uppgifterna blir fler. För att förhindra att uppgifter blir tillgängliga i andra myndigheters verksamhet även i situationer när detta inte är nödvändigt av verksamhetsskäl i det enskilda fallet bör tillgången till automatiserad information begränsas så att endast den som behöver en viss uppgift för att kunna fullgöra sina arbetsuppgifter kan få tillgång till den genom direktåtkomst.

Från brottsbekämpningssynpunkt kan det ibland vara av värde att uppgifter bevaras under en längre tid. För den enskilde kan emellertid ett sådant bevarande innebära att integritetsintrånget består. Att uppgifterna bevaras under lång tid medför också att den totala mängden information om en person kan komma att öka, vilket kan vara negativt från integritetsskyddssynpunkt. Det är därför nödvändigt att utforma den nya lagens bestämmelser om gallring så att personuppgifter inte bevaras under längre tid än vad som behövs.

Några remissinstanser, bl.a. *Kammarrätten i Stockholm, Ekobrottsmyndigheten* och *Rikspolisstyrelsen,* anser att det bör förtydligas att lagens syfte inte endast är att skydda den personliga integriteten vid personuppgiftsbehandling inom polisen utan även att främja en effektiv brottsbekämpning. Som nämnts förutsätter samhällets rättmätiga krav på ett rättssäkert och effektivt brottsbekämpande arbete bl.a. att polisen ges möjlighet att behandla personuppgifter på ett ändamålsenligt sätt med hjälp av väl fungerande informationsteknik. Samtidigt måste skyddet av den enskildes personliga integritet värnas. Båda dessa utgångspunkter är väsentliga för den nya lagen. Som några remissinstanser påpekar bör det i lagen komma till uttryck att dess övergripande syfte inte bara är att skydda den enskildes personliga integritet utan även att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i den brottsbekämpande verksamheten.

6.3 Lagens tillämpningsområde

Regeringens förslag: Den nya lagen ska gälla vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Den personuppgiftsbehandling som sker med stöd av de särskilda lagarna om belastningsregister, misstankeregister, Schengens informationssystem samt passagerarregister ska dock inte omfattas av den nya lagen. Lagen ska inte heller gälla för personuppgiftsbehandling i polisens vapenregister eller i det allmänna spaningsregistret.

Lagen ska innehålla vissa bestämmelser om behandling av uppgifter om juridiska personer.

Utredningens förslag överensstämmer delvis med promemorians. Utredningen föreslår dock inte att lagen ska omfatta polisverksamhet vid Ekobrottsmyndigheten eller behandling av uppgifter om juridiska personer. Utredningen föreslår att lagen, liksom polisdatalagen, ska omfatta all den personuppgiftsbehandling som faller in under 2 § 1–3 polislagen

(1984:387). Utredningen föreslår dock ett generellt undantag för insamling genom bild och ljud.

Remissinstanserna har i huvudsak inte haft någon invändning mot utredningens förslag i denna del. *Rikspolisstyrelsen* har dock ansett att den nya lagen ska omfatta all polisverksamhet enligt 2 § polislagen, dvs. även punkterna 4 och 5.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian undantar dock insamling av personuppgifter genom hemlig teleavlyssning, hemlig teleövervakning, hemlig rumsavlyssning samt allmän och hemlig kameraövervakning från lagens tillämpningsområde. Promemorian behandlar inte frågan om lagens tillämpning på vapenregistren.

Remissinstanserna: Majoriteten av remissinstanserna har inga invändningar mot promemorians förslag. Några remissinstanser, däribland *Kammarrätten i Stockholm* och *Tullverket,* efterlyser dock en närmare motivering till varför insamling av uppgifter genom bl.a. hemliga tvångsmedel har undantagits från lagens tillämpningsområde. *Rikspolisstyrelsen* anser att lagen inte bör gälla vid något slag av insamling av personuppgifter i form av bild och ljud förrän åtgärder vidtagits för att göra uppgifterna tillgängliga i presentabelt skick. Styrelsen anser vidare att beskrivningen i promemorian av polisens brottsbekämpande verksamhet inte är helt korrekt, bl.a. med hänsyn till att polisen inte längre bedriver någon allmän övervakningsverksamhet. *Kustbevakningen* påpekar att det är svårt att dra en gräns mellan ordningshållande uppgifter och brottsbekämpande verksamhet. *Åklagarmyndigheten* och *Rikspolisstyrelsen* ifrågasätter om behandling av uppgifter om juridiska personer ska omfattas av lagen.

Statens kriminaltekniska laboratorium anser att den nya lagen även bör gälla för laboratoriet eftersom myndigheten ingår i polisen. *Säkerhetspolisen* anser att det bör klargöras när myndigheten omfattas av lagens bestämmelser och avstyrker att myndigheten i vissa fall inte direkt anges i bestämmelserna utan i stället har ställning som polismyndighet alternativt Rikspolisstyrelsen.

Skälen för regeringens förslag

Myndigheter som ska omfattas av lagen

Polisdatalagen gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Motsvarande bör gälla för den nya lagen. *Statens kriminaltekniska laboratorium* anser att även laboratoriet bör omfattas av den nya lagen eftersom det ingår i polisen.

Statens kriminaltekniska laboratorium är en del av polisväsendet och är en självständig myndighet med Rikspolisstyrelsen som chefsmyndighet. Laboratoriets huvudsakliga uppdrag är att utföra kriminaltekniska undersökningar som föranleds av misstanke om brott. Myndigheten ansvarar även för forskning, utveckling, information, utbildning samt stöd och service inom hela det kriminaltekniska området. Vid bedömningen av om myndigheten ska omfattas av lagen bör det beaktas dels att verksamheten inte är brottsbekämpande i vedertagen mening, dels att myndighetens

personal inte är polismän utan specialister inom sina respektive verksamhetsområden och inte har traditionella polisiära uppgifter eller befogenheter utan arbetar som en sorts sakkunnigt biträde och expertorgan åt polismyndigheterna. Detta talar emot att laboratoriet ska omfattas av en reglering som motiveras av de särskilda krav som ställs på personuppgiftsbehandling i polisens brottsbekämpande verksamhet. Det är vidare viktigt att betona att när laboratoriet hanterar DNA-registren i egenskap av personuppgiftsbiträde åt Rikspolisstyrelsen är laboratoriet skyldigt att följa aktuella bestämmelser i den nya lagen. Utöver hanteringen av DNA-registren är den personuppgiftsbehandling som sker vid laboratoriet relativt begränsad och åtkomsten till behandlade uppgifter i huvudsak förbehållen dess egen personal. Mot denna bakgrund delar regeringen den bedömning som både Polisdatautredningen och promemorian gör att lagen inte bör omfatta Statens kriminaltekniska laboratorium. Med hänsyn till bl.a. den snabba utvecklingen på området för kriminalteknik kan det emellertid finnas anledning att i ett annat sammanhang överväga behovet av att särskilt författningsreglera personuppgiftsbehandlingen vid laboratoriet.

Säkerhetspolisen anser att det bör tydliggöras vilka av lagens bestämmelser som är tillämpliga på dess verksamhet. Inledningsvis kan konstateras att Säkerhetspolisen utgör en del av Rikspolisstyrelsen. Det saknas därför skäl att särskilt omnämna Säkerhetspolisen i författningstexten annat än när bestämmelserna tar sikte på just den verksamhet som bedrivs där. Behandlingen av personuppgifter vid Säkerhetspolisen bör regleras i ett särskilt kapitel i den nya lagen, vilket utvecklas i avsnitt 16. I bestämmelserna i det kapitlet bör Säkerhetspolisen naturligtvis nämnas särskilt eftersom bestämmelserna endast tar sikte på behandlingen av personuppgifter vid Säkerhetspolisen. I kapitlet bör det hänvisas till övriga bestämmelser i den nya lagen som ska vara tillämpliga på Säkerhetspolisens behandling av personuppgifter.

De kapitel i lagen som reglerar personuppgiftsbehandling vid polisen i övrigt föreslås bl.a. innehålla bestämmelser som reglerar möjligheten att behandla uppgifter för att tillhandahålla information till andra. Det rör sig om bestämmelser om sekundära ändamål, sekretessbrytande bestämmelser och bestämmelser om direktåtkomst. I sådana bestämmelser omnämns mottagande myndigheter, t.ex. de myndigheter som får beviljas direktåtkomst. Eftersom exempelvis en polismyndighet bör kunna lämna ut uppgifter till Rikspolisstyrelsen och bevilja myndigheten direktåtkomst måste Rikspolisstyrelsen anges som mottagare i vissa bestämmelser.

I sådana bestämmelser som reglerar t.ex. vilka myndigheter som kan vara mottagare av personuppgifter saknas det skäl att nämna Säkerhetspolisen särskilt, eftersom den utgör en del av Rikspolisstyrelsen. Av 7 § polislagen följer att när Rikspolisstyrelsen leder polisverksamhet ska vad som i lag eller annan författning föreskrivs om polismyndighet i tillämpliga delar gälla även Rikspolisstyrelsen. Detta innebär att Säkerhetspolisen när den som en del av Rikspolisstyrelsen leder polisverksamhet för att förebygga och avslöja brott omfattas av begreppet polismyndighet i bestämmelser som anger polismyndighet som mottagande myndighet. I författningskommentaren till de aktuella bestämmelserna utvecklas detta ytterligare. I sammanhanget bör understrykas att det är polisen i övrigt,

och inte Säkerhetspolisen, som ska tillämpa de aktuella bestämmelserna och som har att bedöma bl.a. i vilken utsträckning som Säkerhetspolisen ska medges direktåtkomst.

Polisverksamhet som ska omfattas av lagen

I 1 § första stycket polisdatalagen sägs att lagen gäller vid behandling av personuppgifter i polisens verksamhet för att (1) förebygga brott och andra störningar av den allmänna ordningen och säkerheten, (2) övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat, eller (3) bedriva spaning och utredning i fråga om brott som hör under allmänt åtal**.** Lagens tillämpningsområde motsvarar polisens uppgifter som de beskrivs i 2 § 1–3 polislagen. Polisdatalagen omfattar således inte personuppgiftsbehandling inom sådan polisverksamhet som faller under 2 § 4 och 5 polislagen, dvs. verksamhet som består i att lämna allmänheten skydd, upplysningar och annan hjälp samt annan verksamhet som ankommer på polisen enligt särskilda bestämmelser. Sådan personuppgiftsbehandling regleras av bestämmelserna i personuppgiftslagen.

Polisdatautredningen föreslår att den nya lagen ska ha samma tillämpningsområde som polisdatalagen, dvs. omfatta polisens uppgifter som de beskrivs i 2 § 1–3 polislagen. Promemorian väljer en annan lösning och föreslår att lagen ska vara tillämplig i polisens brottsbekämpande verksamhet, vilket enligt promemorian innebär ett något snävare tillämpningsområde än det nuvarande. Ett tredje alternativ skulle kunna vara att låta lagen omfatta all personuppgiftsbehandling i polisens verksamhet.

Vid valet mellan dessa alternativ bör det beaktas vilka omständigheter som gör att personuppgiftslagens allmänna regler inte är ändamålsenliga vid personuppgiftsbehandling i polisiär verksamhet. Här finns det anledning att peka på flera olika förhållanden. För det första är det nödvändigt att i polisiär verksamhet behandla en stor mängd uppgifter som, typiskt sett, är känsliga till sin natur och inte bör ges en vidare spridning. För det andra gör sig särskilt starka samhällsintressen gällande inom delar av polisens verksamhet, vilket medför att sedvanliga avvägningar mellan berörda intressen i viss mån måste göras på ett sätt som tillåter större intrång i integriteten än vad som annars hade kunnat tillåtas. Omständigheter av detta slag kan göra det befogat med särskilda – från personuppgiftslagen avvikande – bestämmelser om personuppgiftsbehandling. Det sagda gäller dock i varierande grad beträffande olika delar av polisens verksamhet. Vidare ska det beaktas att svensk lagstiftning måste vara förenlig med dataskyddsdirektivet inom dess tillämpningsområde. I den utsträckning polisens verksamhet som den beskrivs i 2 § polislagen omfattas av gemenskapsrätten är det därför nödvändigt att säkerställa att lagen uppfyller de krav som direktivet ställer upp. I dataskyddsdirektivets artikel 3.2 undantas från direktivets tillämpningsområde bl.a. behandling av personuppgifter som rör allmän säkerhet, statens säkerhet och statens verksamhet på straffrättens område. För att uppfylla direktivets krav bör personuppgiftslagen tillämpas på verksamhet som inte är undantagen från direktivets tillämpningsområde.

Behovet av en särreglering av behandlingen av personuppgifter är tydligast på det brottsbekämpande området. I annan polisverksamhet, t.ex. tillståndsgivning av olika slag, är behovet av särregler i förhållande till personuppgiftslagen litet eller obefintligt. Det skulle i och för sig ha ett visst praktiskt värde om all personuppgiftsbehandling inom polisen reglerades av en och samma lag, eftersom man därigenom skulle undvika vissa gränsdragningsproblem. Något mer påtagligt behov av en sådan samlad reglering har dock inte framkommit. Det är inte heller säkert att de begränsningar i personuppgiftsbehandlingen som bör finnas i den nya lagen skulle vara ändamålsenliga för all polisiär verksamhet.

Polisdatalagen utgår från 2 § polislagen vid beskrivningen av lagens tillämpningsområde. I den paragrafen finns en uppräkning av polisens uppgifter som tar sin utgångspunkt i polisens funktioner. Vid tillkomsten av 2 § polislagen var målsättningen att beskriva uppgifterna på ett sätt som bättre skulle överensstämma med den verksamhetsplanering som tillämpades inom polisväsendet (prop. 1983/84:111 s. 52). Då indelades polisens arbetsuppgifter i huvuduppgifterna brottsförebyggande verksamhet, övervakningsverksamhet, utredningsverksamhet och serviceverksamhet. Serviceverksamheten kom till uttryck i 2 § 4 och 5 och övrig verksamhet i 2 § 1–3 polislagen.

Även om polisens arbetsuppgifter fortfarande i allt väsentligt är desamma som vid polislagens tillkomst så har beskrivningen av uppgifterna förändrats. Som *Rikspolisstyrelsen* påtalar nämns inte övervakningsverksamhet längre som ett självständigt verksamhetsområde i polisens nuvarande verksamhetsplanering.

Det kan således konstateras att 2 § polislagen bygger på en indelning av polisens verksamhet som polisen delvis har frångått. Detta talar mot att i den nya lagen beskriva lagens tillämpningsområde genom att återge punkterna i 2 § polislagen. Eftersom behovet av särregler i förhållande till personuppgiftslagen är tydligast när det gäller den brottsbekämpande verksamheten bör lagens tillämpningsområde vara behandling av personuppgifter i sådan verksamhet. Motsvarande lösning har valts för Tullverkets brottsbekämpande verksamhet.

Med brottsbekämpande verksamhet avses här verksamhet som syftar till att förebygga, förhindra eller upptäcka brottslig verksamhet eller till att utreda eller beivra brott. Detta bör komma till uttryck i den nya lagens ändamålsbestämmelser. Frågan är då vilka polisuppgifter som ryms inom dessa ändamål och därmed bör anses utgöra brottsbekämpande verksamhet i detta sammanhang. När denna bedömning görs finns det skäl att utgå från beskrivningen av polisens uppgifter i 2 § polislagen, trots att polisen numera tillämpar en något annan indelning av arbetsuppgifterna.

Till de uppgifter som avses i 2 § 4 och 5 polislagen hör bl.a. hjälpåtgärder inom trafiken, medverkan vid katastrofer och liknande händelser, t.ex. biträde enligt räddningstjänstlagen (punkten 4). Hit hör också åliggande av skilda slag inom området för offentlig förvaltning, t.ex. tillstånds- och tillsynsärenden av olika slag (avseende exempelvis vapen, sprängämnen, offentliga tillställningar och nyttjande av offentlig plats), passärenden och ärenden om delgivning eller annan handräckning (punkten 5). Hit räknas även vissa verkställighetsåtgärder på kriminalvårdens och socialtjänstens område. Både Polisdatautredningen och promemorian anser att det i dessa fall inte finns något tydligt behov av särregler

i förhållande till personuppgiftslagen. Några skäl att göra en annan bedömning har inte framkommit. De nämnda verksamheterna kan inte heller i egentlig bemärkelse anses utgöra brottsbekämpande verksamhet och bör således inte omfattas av lagens tillämpningsområde.

Nästa fråga är om personuppgiftsbehandling i anslutning till alla de uppgifter som omfattas av 2 § 1–3 polislagen, i likhet med vad som gäller enligt polisdatalagen, bör omfattas av den nya lagen eller om punkterna inrymmer uppgifter som inte bör betraktas som brottsbekämpande i detta sammanhang.

I 2 § 1 och 2 polislagen används begreppet allmän ordning och säkerhet. Begreppet, som under lång tid har använts i polisförfattningar, är vittomfattande och svårdefinierat. Enligt bestämmelserna kan den allmänna ordningen och säkerheten störas både genom brott och på andra sätt. Sådana polisuppgifter som innebär att polisen förebygger, hindrar och ingriper mot andra störningar av den allmänna ordningen och säkerheten än som innefattar brott kan inte anses utgöra brottsbekämpande verksamhet i det här sammanhanget. Detsamma gäller övervakning av den allmänna ordningen och säkerheten som inte syftar till att förebygga brott. *Rikspolisstyrelsen* framhåller att polisen inte längre bedriver någon allmän övervakningsverksamhet utan att all yttre verksamhet antingen är planlagd brottsförebyggande eller brottsutredande verksamhet.

Trots att polisen inte längre har en särskild verksamhetsgren som benämns övervakning eller ordningshållande verksamhet ingår sådana uppgifter likväl i polisens arbetsuppgifter. De renodlade ordningsuppgifterna är numera inte lika tydliga som förut. Det åligger visserligen polisen att förebygga och ingripa mot störningar av den allmänna ordningen vid stora evenemang, men sådana störningar utgör inte sällan olika straffbara beteenden. Vidare har polisen till uppgift att utföra trafikövervakning, men då i regel med fokus på regelefterlevnad i fråga om bl.a. hastighetsbegränsningar. Utanför det brottsbekämpande området faller däremot uppgiften att planera och övervaka särskilda transporter, t.ex. i samband med statsbesök. Det ligger i sakens natur, som *Kustbevakningen* påpekar, att det är svårt att dra en tydlig gräns mellan ordningshållande uppgifter och brottsbekämpning. Detta beror på att övervakning och ordningshållande verksamhet även kan syfta till att förebygga och ingripa mot brott samt att sådan verksamhet ofta kan övergå i brottsbekämpning. Vid en slumpvis utförd trafiknykterhetskontroll, som ju i någon mening också är brottsförebyggande, kan exempelvis misstanke om brott eller brottslig verksamhet uppstå liksom vid polisens ordningshållande arbete under stora evenemang. Det skulle dock föra för långt att hävda att den mer renodlade övervakning och ordningshållande verksamhet som polisen bedriver ska betraktas som brottsbekämpande och därmed omfattas av en ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Av det sagda framgår att vissa gränsdragningsproblem mellan brottsbekämpande och icke brottsbekämpande verksamhet kan uppstå, men dessa ska inte överdrivas. Polisen måste alltid i sitt arbete i det enskilda fallet ta ställning till syftet med pågående verksamhet eftersom detta har betydelse för vilka befogenheter polisen har enligt bl.a. bestämmelserna i 10–24 d §§ polislagen.

Vissa uppgifter som omfattas av 2 § 1–3 polislagen kan således inte anses utgöra brottsbekämpande verksamhet och bör därmed inte omfattas av den nya lagens tillämpningsområde.

Personuppgiftsbehandling med stöd av särskilda författningar

Utgångspunkten är att den nya lagen ska omfatta all behandling av personuppgifter i polisens brottsbekämpande verksamhet. Undantag bör emellertid göras för vissa register.

Som både Polisdatautredningen och promemorian föreslår bör den nya lagen inte omfatta personuppgiftsbehandling som sker med stöd av lagarna om belastningsregister, misstankeregister, Schengens informationssystem samt passagerarregister. Dessa lagar har väl avgränsade tillämpningsområden och några påtagliga tillämpningssvårigheter eller problem med en särreglering har inte framkommit. Inte heller polisdatalagen omfattar personuppgiftsbehandling med stöd av nämnda författningar.

Varken Polisdatautredningen eller promemorian behandlar frågan om den nya lagens tillämpning på polisens vapenregister som förs med stöd av 2 kap. 17–21 §§ vapenlagen (1996:67). Enligt 2 kap. 20 § vapenlagen ska vapenregistren ha till ändamål att dels ge information om sådana uppgifter som behövs för att förebygga, upptäcka och utreda brott med anknytning till skjutvapen, dels att underlätta handläggningen av frågor om tillstånd enligt vapenlagen. Registren förs således delvis för brottsbekämpande ändamål. I förarbetena till bestämmelserna gjordes därför bedömningen att – utöver personuppgiftslagen – polisdatalagens allmänna bestämmelser skulle gälla för behandlingen av personuppgifter i registren (prop. 1998/99:36 s. 12 och 20). I propositionen uttalades att detta i praktiken endast skulle innebära att vissa av polisdatalagens bestämmelser om uppgiftsskyldighet och utlämnande av uppgifter skulle bli tillämpliga (a. prop. s. 20).

Det saknas skäl att föreslå någon materiell förändring av regleringen av vapenregistren. En annan och tydligare lagteknisk konstruktion bör dock väljas. De huvudsakliga bestämmelserna om vapenregistren bör även fortsättningsvis finnas i vapenlagen och kompletteras av bestämmelserna i personuppgiftslagen. Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör inte gälla för behandlingen av personuppgifter i vapenregistren annat än om en särskild hänvisning till den lagen görs i vapenlagen. För att åstadkomma en överensstämmelse med vad som redan gäller bör det i vapenlagen tas in en sådan hänvisning till de bestämmelser i den nya lagen om uppgiftsskyldighet och utlämnande av uppgifter som motsvarar gällande reglering.

Andra register som inte heller behandlas av Polisdatautredningen eller promemorian är registret över förelägganden av ordningsbot och registret över uppbörd i ärenden om strafföreläggande. Dessa register förs av Rikspolisstyrelsen med stöd av förordningen (1997:903) om register över förelägganden av ordningsbot respektive förordningen (1997:902) om register över strafföreläggande och utgör huvudsakligen ett stöd för polisen vid verkställighet av påföljderna föreläggande av ordningsbot och strafföreläggande. Registren har således primärt ett annat ändamål än

brottsbekämpning och faller därmed utanför den nya lagens tillämpningsområde.

Den nya lagen bör inte heller omfatta behandling av personuppgifter i polisens allmänna spaningsregister. Den frågan behandlas i avsnitt 19.

Insamling genom bild- och ljudupptagning

Promemorian föreslår ett undantag från den nya lagens tillämpningsområde vad gäller insamling av personuppgifter genom hemlig teleavlyssning, hemlig teleövervakning, hemlig rumsavlyssning samt allmän och hemlig kameraövervakning. Bl.a. *Kammarrätten i Stockholm* och *Tullverket* efterlyser skälen för undantaget. *Rikspolisstyrelsen* anser att undantaget bör utsträckas till att gälla all insamling av personuppgifter i form av bild och ljud och hänvisar till att Polisdatautredningen föreslår ett sådant generellt undantag. Styrelsen pekar särskilt på några bestämmelser i promemorians förslag som skulle bli svåra att tillämpa vid sådan insamling. Som exempel nämner styrelsen att personuppgifter som görs eller har gjorts gemensamt tillgängliga ska förses med en särskild upplysning om det närmare ändamålet med behandlingen och om personen som uppgiften avser inte är misstänkt för visst brott eller för att ha utövat eller för att komma att utöva allvarlig eller systematisk brottslig verksamhet.

Inledningsvis kan det konstateras att promemorians förslag skiljer sig från Polisdatautredningens bl.a. vad gäller uppdelningen mellan gemensamt tillgängliga uppgifter och andra uppgifter. Enligt promemorians förslag torde insamlingen av uppgifter och den initiala lagringen av materialet i regel komma att omfattas endast av de grundläggande dataskyddsbestämmelserna och inte av de mer begränsande bestämmelserna om gemensamt tillgängliga uppgifter. Starka skäl talar för att de grundläggande dataskyddsbestämmelserna bör gälla även vid insamling av uppgifter. Uppgifter bör t.ex. bara få behandlas om det är lagligt, om det sker på ett korrekt sätt och fler uppgifter bör inte få samlas in än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det ökade integritetsskydd som uppnås genom att låta lagens bestämmelser också gälla för insamlingen av uppgifter uppväger de eventuella problem som kan uppstå för polisen i fråga om polisens möjligheter att använda digital teknik. Något *generellt* undantag för insamling av uppgifter genom bild- och ljudupptagning bör således inte införas. Som Rikspolisstyrelsen förordar bör dock bestämmelsen i 23 § personuppgiftslagen (1998:204), som föreskriver en skyldighet att informera den person som uppgifter samlas in från om behandlingen, inte gälla vid sådan insamling. Den frågan behandlas i avsnitt 6.4.2. Rikspolisstyrelsen anför även synpunkter på svårigheten att tillämpa bestämmelserna om särskilda upplysningar och gallring på bild- och ljudupptagningar. Dessa frågor tas upp i avsnitt 10 och 14.3.

När det gäller insamling av personuppgifter genom hemlig teleavlyssning, hemlig teleövervakning, hemlig rumsavlyssning samt allmän och hemlig kameraövervakning finns särskilda bestämmelser i rättegångsbalken, lagen (1998:150) om allmän kameraövervakning, lagen (2007:978) om hemlig rumsavlyssning, lagen (2007:979) om åtgärder för att förhind-

ra vissa särskilt allvarliga brott och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott. Särskilda bestämmelser finns dessutom i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Nämnda författningar reglerar framför allt förutsättningarna för insamlingen av uppgifter men det finns även bestämmelser som begränsar användningen av de insamlade uppgifterna, bl.a. användningen av överskottsinformation. Bestämmelserna i de aktuella lagarna syftar till att värna den enskildes integritet vid användningen av hemliga tvångsmedel och allmän kameraövervakning. Det behövs dock kompletterande integritetsskyddande bestämmelser som tar sikte på behandlingen av personuppgifter. Behovet av sådana kompletterande bestämmelser synes emellertid inte vara särskilt stort vad gäller den del av behandlingen som avser insamlingen av uppgifter, eftersom bestämmelserna i den särskilda lagstiftningen är detaljerade i detta avseende. Detta talar i och för sig för att undanta insamlingen från den nya lagens tillämpningsområde, vilket också föreslås i promemorian. Eftersom den särskilda lagstiftningen på området har andra syften och inte i alla avseenden beaktar de integritetsaspekter som den nya lagen ska värna, bör emellertid även insamlingen av uppgifter genom hemliga tvångsmedel och, i förekommande fall, allmän kameraövervakning omfattas av den nya lagen. Insamlingen av uppgifter genom hemlig teleövervakning, hemlig teleavlyssning, hemlig rumsavlyssning samt allmän och hemlig kameraövervakning bör därför inte undantas från den nya lagens tillämpningsområde. Något sådant undantag finns inte heller i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Juridiska personer

I promemorian föreslås att behandling av uppgifter om juridiska personer ska omfattas av vissa grundläggande bestämmelser i den nya lagen, bl.a. bestämmelserna om tillåtna ändamål, sökbegränsningar och gallring. Motsvarande bedömning gjordes vid tillkomsten av lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (se prop. 2004/05:164 s. 55). Några remissinstanser ifrågasätter dock om ett av huvudsyftena med den nya lagstiftningen, nämligen att skydda den personliga integriteten, verkligen gör sig gällande i fråga om juridiska personer. *Rikspolisstyrelsen* pekar på att juridiska personer ofta används som brottshjälpmedel och att det därför bl.a. är viktigt att kunna söka på firma eller organisationsnummer för att hitta företag som kan antas ha samband med brottslig verksamhet. Även om juridiska personer inte har samma behov av integritetsskydd som fysiska personer bör enligt regeringens mening vissa grundläggande bestämmelser tillämpas även på juridiska personer. Det kan dessutom vara svårt att i den elektroniska hanteringen skilja uppgifter om juridiska personer från uppgifter om fysiska personer som är ägare av eller ställföreträdare för dessa. Starka verksamhetsskäl talar dock för att undanta juridiska personer från bestämmelserna om sökbegränsningar. Den frågan tas upp i avsnitt 11.

6.4 Den nya lagen och personuppgiftslagen

6.4.1 Förhållandet till personuppgiftslagen

Regeringens förslag: Den nya lagen ska gälla i stället för personuppgiftslagen. I lagen hänvisas till de bestämmelser i personuppgiftslagen som ska gälla vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Utredningens förslag: Den nya lagen ska vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som ska tillämpas i polisens verksamhet.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt förslaget eller inte haft någon invändning mot det. Dåvarande *Kriminalvårdsstyrelsen* har ställt sig tveksam till förslaget och menat att det är lämpligare att den nya lagen endast hänvisar till personuppgiftslagen. *Statskontoret* har uttalat att förhållandet mellan personuppgiftslagen och den föreslagna polisdatalagen inte är tillräckligt utrett. *Riksarkivet* har ansett att bestämmelserna i personuppgiftslagen, som riktar sig mot en stor krets av behandlingar inom skilda verksamhetsgrenar, kan bli missvisande om de rakt av överförs till en så speciell verksamhet som polisens. Dåvarande *Riksskatteverket* har ansett att lagen bör hänvisa till bestämmelserna i personuppgiftslagen, i stället för att upprepa dem. *Kammarrätten i Jönköping* och *Sveriges Domareförbund* har förordat en lagstiftningsteknik som innebär att de bestämmelser som avviker från personuppgiftslagen regleras särskilt i den nya lagen och att det tydligt i denna hänvisas till de lagrum i personuppgiftslagen som är tillämpliga.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag: Personuppgiftslagen bygger, som nämnts i avsnitt 4.2.5, på EG:s dataskyddsdirektiv och är generellt tillämplig på behandling av personuppgifter. Eftersom direktivet bl.a. inte omfattar behandling av personuppgifter som utförs på området för statens brottsbekämpande verksamhet, finns det ur EG-rättslig synvinkel i och för sig inte något som hindrar att den nya lagen utformas på annat sätt än vad som anges i dataskyddsdirektivet. I sammanhanget kan dock påpekas att direktivet i huvudsak bygger på och vidareutvecklar de bestämmelser som finns i dataskyddskonventionen. Konventionen gäller även i statens brottsbekämpande verksamhet. Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. Vidare bör beaktas att dataskyddsrambeslutet, som snart ska genomföras, i stora delar liknar dataskyddsdirektivet.

Trots att EG:s dataskyddsdirektiv formellt inte är tillämpligt i fråga om behandling av personuppgifter i den brottsbekämpande verksamheten bör enligt regeringens mening en reglering som avviker från de grundläggande reglerna i personuppgiftslagen införas bara om det finns goda skäl för det. Systematiska skäl talar också för att den nya regleringen bör ansluta till personuppgiftslagen. Det är således önskvärt att de bestämmelser till skydd för enskilds integritet som uppställs i personuppgiftslagen så långt

möjligt tillämpas även vid personuppgiftsbehandling inom polisens brottsbekämpande verksamhet.

Med hänvisning till det som sagts ovan bör personuppgiftslagens bestämmelser i väsentliga delar gälla även i polisens brottsbekämpande verksamhet. I denna verksamhet finns emellertid särskilda behov av att kunna behandla personuppgifter automatiserat och verksamhetens särdrag gör dessutom att personuppgiftslagens bestämmelser inte alltid är ändamålsenliga. I vissa delar bör det därför införas bestämmelser som avviker från den lagen.

Hur bör då de regler i personuppgiftslagen som ska gälla även i polisens brottsbekämpande verksamhet infogas i det nya regelverket? I tidigare lagstiftningsärenden, där motsvarande fråga har uppkommit, har olika lösningar valts. En modell har varit att i den författning som reglerar behandling av personuppgifter i en viss verksamhet över huvud taget inte nämna personuppgiftslagen. Det innebär att personuppgiftslagens bestämmelser utan vidare kommer att vara tillämpliga, i den mån den särskilda författningen inte innehåller avvikande bestämmelser (se 2 § personuppgiftslagen). En liknande modell, som ger samma effekt, är att i den särskilda författningen ange att den gäller utöver personuppgiftslagen. Den modellen används i bl.a. polisdatalagen. Nackdelen med båda dessa lösningar är att det kan vara svårt att överblicka vilka bestämmelser i personuppgiftslagen som är tillämpliga.

Polisdatautredningen föreslår en annan modell. Förslaget innebär att den nya lagen ska vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som ska gälla för polisen. En liknande lösning har valts för personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (prop. 2006/07:46; SFS 2007:258 och 2007:259). Fördelen med en sådan lösning är att tillämparen snabbt får klart för sig vilka bestämmelser som gäller utan att behöva gå till personuppgiftslagen. En nackdel är dock att det i viss mån blir fråga om en dubbelreglering, eftersom personuppgiftslagens bestämmelser ändå gäller om inget annat anges. En annan nackdel är att lagen blir omfattande.

Ytterligare en annan lösning har valts i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Lagen innehåller, utöver de bestämmelser som avviker från personuppgiftslagen, en hänvisning till de lagrum i personuppgiftslagen som är tillämpliga. Lagrådet hade inte några invändningar mot den valda metoden. Samma lösning har nyligen också föreslagits för Kustbevakningens personuppgiftsbehandling (SOU 2006:18) och för åklagarväsendets personuppgiftsbehandling (SOU 2008:87). Fördelarna med en sådan lösning är att lagstiftningen blir mer överskådlig, tydlig och lättillämpad jämfört med om inga hänvisningar görs till personuppgiftslagen. Samtidigt undviks en omfattande dubbelreglering.

Utvecklingen går mot ökat samarbete mellan de brottsbekämpande myndigheterna. Det ligger därför ett värde i att så långt möjligt använda samma lagstiftningsteknik för all behandling av personuppgifter inom den brottsbekämpande verksamheten, oavsett myndighet. Den nya lagen bör, mot bakgrund av det sagda, gälla i stället för personuppgiftslagen och innehålla tydliga hänvisningar till tillämpliga lagrum i den lagen.

6.4.2 Tillämpliga bestämmelser i personuppgiftslagen

Regeringens förslag: Följande bestämmelser i personuppgiftslagen ska vara tillämpliga vid behandling av personuppgifter i polisens brottsbekämpande verksamhet:

– definitioner (3 §),
– förhållandet till offentlighetsprincipen m.m. (8 §),
– grundläggande krav på behandling (9 §, med undantag för vad som anges i paragrafens första stycke i och tredje stycket),
– behandling av personnummer (22 §),
– information till den registrerade (23 och 25–27 §§),
– rättelse (28 §),
– säkerheten vid behandling (30 och 31 §§ samt 32 § första stycket),
– överföring av personuppgifter till tredjeland (33–35 §§),
– personuppgiftsombudets uppgifter m.m. (38–41 §§),
– upplysningar till allmänheten om vissa behandlingar (42 §),
– tillsynsmyndighetens befogenheter (43, 44 §§, 45 § första stycket och 47 §),
– skadestånd (48 §), och
– överklagande (51 § första stycket, 52 § första stycket och 53 §).

Bestämmelserna i 8 § andra stycket personuppgiftslagen ska dock inte tillämpas om personuppgifter ska gallras enligt bestämmelser i den nya lagen eller enligt föreskrifter som meddelats i anslutning till lagen.

Bestämmelserna om informationsskyldighet i 23 § personuppgiftslagen behöver inte tillämpas om uppgifterna samlas in

1. genom bild- eller ljudupptagning eller
2. i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Tillsynsmyndigheten ska inte kunna förena ett förbud att utföra viss behandling med vite.

Utredningens förslag överensstämmer i huvudsak med promemorians.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt förslaget eller inte haft några invändningar mot det.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår dock inte något undantag från informationsplikten i 23 § personuppgiftslagen i fråga om insamling genom bild- eller ljudupptagning. Promemorian föreslår inte heller att någon hänvisning görs till 9 § första stycket c eller d, eller till andra och fjärde styckena.

Remissinstanserna: En majoritet av remissinstanserna instämmer i eller har inget att invända mot promemorians förslag. *Rikspolisstyrelsen* anser dock att bl.a. skyldigheten att lämna information enligt 23, 25 och 26 §§ personuppgiftslagen kommer att försvåra för polisen att använda digital teknik vid insamling av uppgifter. Styrelsen anser att samma regler bör gälla vid insamling av bilder och ljud, oavsett om upptagningarna sker med analog eller digital utrustning. Rikspolisstyrelsen anser vidare att polisen alltid bör få behandla personuppgifter för historiska, vetenskapliga och statistiska ändamål och föreslår därför att den nya lagen även bör hänvisa till 9 § andra–fjärde styckena personuppgiftslagen. Styrelsen gör bedömningen, bl.a. mot bakgrund av hänvisningen i pro-

memorians lagförslag till 8 § personuppgiftslagen, att utgallrade uppgifter torde kunna föras över till ett digitalt arkiv och där behandlas för de ändamål som anges i arkivlagen (1990:782). *Datainspektionen* påpekar att det av dataskyddskonventionen följer att insamlade uppgifter aldrig får användas på ett sätt som är oförenligt med det eller de specifika ändamål för vilket de samlades in (den s.k. finalitetsprincipen). Enligt Datainspektionen strider promemorians lagförslag på denna punkt mot konventionens krav. Inspektionen anser därför att det i den nya lagen bör införas en generell regel som upprätthåller finalitetsprincipen, exempelvis genom att en hänvisning görs till 9 § första stycket d personuppgiftslagen. Datainspektionen framhåller att det är positivt att tillsynsmyndigheten föreslås ha i stort sett identiska befogenheter vid tillsynen över polisens här aktuella personuppgiftsbehandling som enligt personuppgiftslagen. *Kammarrätten i Stockholm* menar att 22 § personuppgiftslagen bör vara tillämplig endast när uppgifterna behandlas på annat sätt än när de görs eller har gjorts gemensamt tillgängliga.

Skälen för regeringens förslag

Redan nu tillämpas många av personuppgiftslagens bestämmelser i polisens personuppgiftsbehandling, eftersom polisdatalagen gäller utöver personuppgiftslagen. Förslaget innebär få förändringar i detta hänseende men en tydligare reglering. Nedan redovisas i vilken utsträckning personuppgiftslagens bestämmelser bör vara tillämpliga vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Definitioner (3 §)

I 3 § personuppgiftslagen definieras vissa begrepp som är centrala vid behandling av personuppgifter. Där definieras t.ex. vad personuppgifter är (”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.”) och vad som utgör behandling av personuppgifter (”Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.”). Definitionerna gäller också för personuppgiftsbehandling som sker med stöd av polisdatalagen. Det finns inte skäl att göra någon ändring i detta hänseende. Det är viktigt att terminologin i den nya lagen överensstämmer med personuppgiftslagens och att de begrepp som används i de båda författningarna har samma innebörd. En hänvisning till 3 § personuppgiftslagen bör därför tas in i den nya lagen.

Förhållandet till offentlighetsprincipen (8 §)

I 8 § första stycket personuppgiftslagen erinras om att personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att lämna ut personuppgifter enligt 2 kap. tryckfrihets-

förordningen, som reglerar allmänna handlingars offentlighet. I paragrafens andra stycke anges att bestämmelserna inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Paragrafen gäller för personuppgiftsbehandling hos polisen.

I klargörande syfte bör en hänvisning till bestämmelserna i 8 § personuppgiftslagen tas in i den nya lagen. Det bör dock tydliggöras att bestämmelserna i 8 § andra stycket inte är tillämpliga när uppgifter ska gallras enligt särskilda bestämmelser i den nya lagen. Utgallrade uppgifter bör inte, till skillnad från hur *Rikspolisstyrelsen* har tolkat de föreslagna bestämmelserna, få bevaras i ett digitalt arkiv och vara åtkomliga för arkivändamål. Sådant bevarande kommer att vara tillåtet endast om det meddelas föreskrifter med undantag från den nya lagens gallringsbestämmelser som tillåter ett bevarande. Den frågan tas upp i avsnitt 14.1.

Grundläggande krav på behandlingen av personuppgifter (9 §)

Några av personuppgiftslagens viktigaste bestämmelser om behandling av personuppgifter finns i 9 §. Där uppställs vissa grundläggande krav på den personuppgiftsansvarige. I första stycket a och b anges att den personuppgiftsansvarige ska se till att personuppgifter endast behandlas om det är lagligt och att personuppgifter alltid ska behandlas på ett korrekt sätt och i enlighet med god sed. Enligt e–h ska den ansvarige se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen, att inte fler personuppgifter behandlas än som är nödvändigt, att de personuppgifter som behandlas är riktiga och om nödvändigt aktuella samt att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Det är naturligt att dessa krav tillämpas även vid behandling av personuppgifter inom polisens brottsbekämpande verksamhet. Den nya lagen bör därför hänvisa till 9 § första stycket a, b och e–h personuppgiftslagen.

I 9 § första stycket c anges att personuppgifter får samlas in bara för särskilda, uttryckligt angivna ändamål och i punkten d att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. En skyldighet för polisen att ha ett preciserat ändamål för insamlingen av personuppgifter kan sägas följa redan av de materiella bestämmelser om t.ex. förundersöknings bedrivande som styr polisens verksamhet. För att tydliggöra kravet på att personuppgifter får samlas in endast för preciserade ändamål bör det emellertid tas in en hänvisning till 9 § första stycket c personuppgiftslagen i den nya lagen.

Punkten d ger uttryck för den s.k. finalitetsprincipen. *Datainspektionen* anser att 9 § första stycket d bör vara tillämplig även vid behandling i polisens brottsbekämpande verksamhet. I promemorian föreslås att det i den nya lagen inte bör tas in någon hänvisning till finalitetsprincipen. I stället bör den nya lagen uttömmande ange för vilka ändamål uppgifter får behandlas i polisens brottsbekämpande verksamhet. Denna verksamhet är emellertid omfattande och innehåller arbetsuppgifter av vitt skilda

slag. Det är därför svårt att i alla avseenden kunna bedöma nuvarande behov av personuppgiftsbehandling och att förutse alla de behov av sådan behandling som kan göra sig gällande i framtiden. Det finns därför enligt regeringens mening skäl att göra en hänvisning till 9 § första stycket d personuppgiftslagen. Frågan behandlas närmare i avsnitt 7.1.

Rikspolisstyrelsen menar att 9 § andra–fjärde styckena bör vara tillämpliga vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet. Enligt paragrafens andra stycke gäller att behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål generellt inte ska anses som oförenlig med de ändamål för vilka uppgifterna samlades in. I paragrafens fjärde stycke föreskrivs begränsningar i fråga om behandlingen av uppgifter som bevarats för historiska, statistiska och vetenskapliga ändamål. Dessa bestämmelser bör gälla även i polisens brottsbekämpande verksamhet. I 9 § första stycket i och tredje stycket personuppgiftslagen finns bestämmelser om hur länge uppgifter får bevaras. Frågan om gallring och bevarande av uppgifter bör regleras särskilt i den nya lagen. Någon hänvisning till personuppgiftslagens bestämmelser i 9 § första stycket i och i tredje stycket om hur länge uppgifter får bevaras behövs därför inte. Frågan behandlas i avsnitt 14.

Behandling av personnummer (22 §)

I 22 § personuppgiftslagen föreskrivs att uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Personnummer bör således inte användas av ren slentrian. Bestämmelserna innebär att den personuppgiftsansvarige måste göra en intresseavvägning. Tyngden av de skäl som talar för att behandlingen av personnummer är påkallad måste således vägas mot behovet av skydd för den personliga integriteten. Principen bör enligt regeringens mening gälla även vid behandling i polisens brottsbekämpande arbete. Av integritetsskäl kan det många gånger vara nödvändigt att använda personnummer med hänsyn till den större säkerhet för en riktig identifiering som detta innebär, särskilt i polisens verksamhet. Till skillnad från vad *Kammarrätten i Stockholm* anser finns det inte skäl att göra avsteg från principen i fråga om gemensamt tillgängliga uppgifter, även om det vid behandling av sådana uppgifter i många fall är nödvändigt att behandla personnummer. Den nya lagen bör därför hänvisa även till 22 § personuppgiftslagen.

Information till den registrerade (23 och 25–27 §§)

Allmänt

Personuppgiftslagens bestämmelser om sådan information som ska lämnas självmant till den registrerade och om information som ska lämnas efter ansökan av den registrerade (23 och 25–27 §§) tillämpas enligt gällande reglering vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Av 23 § personuppgiftslagen följer att den personuppgiftsansvarige självmant ska informera en enskild om behandling av uppgifter som samlas in från den enskilde själv. Den information som ska lämnas är enligt 25 § uppgift om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter. Information behöver dock inte lämnas om sådant som den registrerade redan känner till. Information ska också, enligt 26 § personuppgiftslagen, lämnas på begäran av den registrerade. Om uppgifter behandlas ska information lämnas till sökanden om vilka uppgifter det rör sig om, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Under förutsättning att uppgifterna inte har lämnats ut till tredje man behöver dock information inte lämnas om personuppgifter i löpande text som inte har fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. I 26 § finns även bestämmelser om inom vilken tid en ansökan ska besvaras. Enligt 27 § personuppgiftslagen gäller inte rätten till information om det i lag eller annan författning eller i beslut som har meddelats med stöd av författning särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade. Information behöver alltså inte lämnas om sådana förhållanden för vilka det gäller sekretess.

Bestämmelserna utgör i allt väsentligt en lämplig avvägning mellan den enskildes intresse av att få information om behandling av uppgifter om denne och polisens intresse av effektiva medel för brottsbekämpning. En hänvisning till bestämmelserna bör därför införas i den nya lagen. Det bör dock övervägas om det i den nya lagen behövs undantag från informationsskyldigheten för viss insamling av uppgifter som t.ex. insamling genom bild och ljud och insamling i samband med larm.

Undantag för insamling genom bild och ljud

Rikspolisstyrelsen anser att bestämmelserna i 23, 25 och 26 §§ personuppgiftslagen är svåra att tillämpa när uppgifter samlas in genom bild- och ljudupptagning och menar att samma regler bör gälla oavsett om upptagningarna sker med analog eller digital utrustning. Som redovisas i avsnitt 6.3 bör lagen som huvudregel vara tillämplig även på insamling genom bild och ljud. Det finns dock skäl att överväga om det kan krävas att informationsskyldigheten ska fullgöras fullt ut vid sådan insamling. Inledningsvis kan konstateras att polisens möjlighet att samla in uppgifter genom bild och ljud i stor utsträckning är oreglerad. De bestämmelser som finns reglerar insamling genom hemliga tvångsmedel, t.ex. reglerna i 27 kap. rättegångsbalken och lagen om hemlig rumsavlyssning. Vidare finns bestämmelser om insamling genom allmän kameraövervakning i lagen (1998:150) om allmän kameraövervakning och bestämmelser i 28 kap. 14 § rättegångsbalken om fotografering av anhållna och häktade. Enligt den paragrafen får även andra personer än anhållna och häktade fotograferas, om det behövs för utredning av brott på vilket fängelse kan följa. I flera betänkanden har föreslagits att polisens möjlighet att använda spaningsmetoder som t.ex. innebär användning av handmanövrerade kameror, dolda kroppsmikrofoner, inspelning av telefonsamtal och

positionsbestämning bör författningsregleras (se t.ex. SOU 2003:74 och 2007:22). Bestämmelser om behandlingen av personuppgifter kan begränsa möjligheten att samla in uppgifter genom bild- och ljudupptagning. Det ligger dock inte inom ramen för detta lagstiftningsärende att överväga när sådan insamling bör få ske. Regeringen har uppdragit åt Polismetodutredningen att överväga bl.a. frågan om författningsreglering av tekniska spaningsmetoder (dir. 2007:185). Även lagen om allmän kameraövervakning är föremål för utredning (dir. 2008:22).

Frågan är om det behövs några undantag från bestämmelserna om informationsskyldighet i 23 och 25–27 §§ personuppgiftslagen för behandling av bild- och ljudupptagningar. Vad gäller 23 § torde i regel något av undantagen i 25 eller 27 § vara tillämpligt på sådan insamling. När en anhållen eller häktad fotograferas i samband med att fingeravtryck tas eller när skador på ett brottsoffer dokumenteras torde exempelvis undantaget i 25 § andra stycket vara tillämpligt. Det måste nämligen förutsättas att den fotograferade känner till varför insamling sker och att den sker genom automatiserad behandling samt att han eller hon förstår vad uppgifterna ska användas till. Vidare torde undantaget i 27 § vanligtvis vara tillämpligt när insamling sker för spaningsändamål inom ramen för en förundersökning eller i underrättelseverksamhet, eftersom sekretess enligt 18 kap. 1 eller 2 § offentlighets- och sekretesslagen normalt gäller i dessa fall. Detsamma gäller insamling genom hemliga tvångsmedel. Det förekommer dock situationer då polisen synes vara skyldig att lämna information enligt 23 § personuppgiftslagen. Exempelvis torde sådan skyldighet föreligga när polisen genom videofilmning öppet dokumenterar ett visst händelseförlopp, t.ex. på grund av oroligheter i samband med en fotbollsmatch. I en sådan situation framstår det emellertid inte bara som orimligt utan också som praktiskt ogörligt att informera alla personer som kan tänkas fångas på bild om att deras personuppgifter behandlas. Värdet av sådan information kan också ifrågasättas. Mot denna bakgrund bör det inte krävas att polisen tillämpar 23 § personuppgiftslagen vid insamling av personuppgifter genom bild och ljud. I sammanhanget kan erinras om undantaget i 5 a § personuppgiftslagen för behandling av personuppgifter i ostrukturerat material som infördes genom en lagändring år 2007 (prop. 2005/06:173).

Däremot finns det inte skäl att göra något undantag från bestämmelserna i 26 § personuppgiftslagen, vilket Rikspolisstyrelsen förespråkar. Bestämmelserna i den paragrafen tar sikte på den fortsatta behandlingen av personuppgifter sedan de har samlats in. Ett grundläggande krav i den nya lagen bör vara att polisen alltid ska veta för vilket ändamål en uppgift bevaras. För att kunna uppfylla detta krav måste polisen känna till det huvudsakliga innehållet av en bild- eller ljudsekvens som bevaras, t.ex. vilken person som spaningen eller brottsutredningen avsåg. Det ligger i sakens natur att polisen inte kan förväntas känna till och dokumentera identiteten på samtliga personer som förekommer i en filmsekvens t.ex. från en allmän plats. Och det faller på sin egen orimlighet att polisen skulle behöva informera samtliga dessa personer om behandlingen. Det bör framhållas – som uttalas i förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 82 f.) – att den personuppgiftsansvarige bara är skyldig att utnyttja de sök- och sammanställningsmöjligheter som han eller hon har tillgång till för att få fram information att lämna till den

registrerade. I sammanhanget kan erinras om att regeringen i nyssnämnda proposition hänvisade till Datalagskommitténs uttalande att ”inte ens EG-rätten kan tvinga någon att göra det som i praktiken är omöjligt” (SOU 1997:39 s. 392). Informationskravet i 26 § torde således inte bli så omfattande som Rikspolisstyrelsen synes befara.

Undantag för insamling i samband med larm

Av Datainspektionens allmänna råd om information till registrerade enligt personuppgiftslagen framgår att information enligt 23 § personuppgiftslagen bör lämnas muntligen när personuppgifter samlas in vid telefonkontakt eller annan muntlig kontakt. Det skulle uppstå praktiska svårigheter om det infördes en skyldighet att lämna uppgifter om behandlingarna av personuppgifter i kommunikationscentralernas system (KC-systemet) till en enskild person i samband med att han eller hon larmar polisen. När en person larmar eller på liknande sätt tillkallar polisen rör det sig typiskt sett om en brådskande situation som kräver omedelbar åtgärd. Både med hänsyn till risken för försening av den åtgärd som efterfrågas i det enskilda fallet och till risken för negativa konsekvenser i stort för verksamheten vid en kommunikationscentral är det orimligt att kräva att polisen lämnar information i samband med larm. I en larmsituation torde den enskilde inte heller finna behovet av sådan information särskilt angelägen. Information som inte uppfattas som relevant i en akut situation kan tvärtom tas emot negativt.

Utredningen om Kustbevakningens personuppgiftsbehandling anser att det inte är nödvändigt med några författningsförslag för att information inte ska behöva lämnas i nu aktuella fall (SOU 2006:18 s. 235). Som skäl anförs att alla som vänder sig till en myndighet i en sådan situation redan känner till att uppgifter registreras i någon form av automatiserat register. Även om undantaget i 25 § andra stycket personuppgiftslagen vanligtvis torde vara tillämpligt finns det ändå skäl att införa ett undantag som tar sikte just på larmsituationer bl.a. av det skälet att larm utgör en stor och viktig del av polisens verksamhet. Det bör i en lagregel klart framgå att information aldrig ska behöva lämnas vid larm om det med hänsyn till omständigheterna inte finns tid att lämna informationen. Bedömningen av om information ska lämnas bör göras från fall till fall. I sådan verksamhet som uteslutande består i att ta emot larm torde det endast undantagsvis finnas tid att lämna information om behandling av personuppgifter.

Rättelse (28 §)

I 28 § personuppgiftslagen anges att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte behandlats i enlighet med personuppgiftslagens bestämmelser. När en personuppgiftsansvarig rättar en personuppgift, ska underrättelse lämnas till tredje man som har fått del av uppgiften, om den registrerade begär det eller om mer betydande skada eller olägenhet därigenom kan undvikas. Sådan underrättelse behöver dock inte lämnas om det visar sig vara omöjligt eller om det skulle innebära en opropor-

tionerligt stor arbetsinsats. Dessa bestämmelser gäller vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet.

Det är viktigt att personuppgifter som behandlas felaktigt hos en myndighet rättas. Bedömningen av om en uppgift har behandlats på ett felaktigt sätt måste göras mot bakgrund av de bestämmelser som gäller för behandlingen, oavsett om det är grundläggande regler i personuppgiftslagen eller specialbestämmelser för polisens verksamhet. Mot bakgrund av det sagda bör bestämmelserna i 28 § personuppgiftslagen även i fortsättningen tillämpas vid behandling av personuppgifter i polisens brottsbekämpande verksamhet. I den nya lagen bör det alltså tas in en hänvisning till 28 § personuppgiftslagen.

Säkerheten vid behandling (30–32 §§)

I 30–32 §§ personuppgiftslagen finns bestämmelser om hur den personuppgiftsansvarige ska organisera arbetet med behandling av personuppgifter för att garantera säkerheten. Dessa bestämmelser är tillämpliga vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet och de bör gälla där även fortsättningsvis. En hänvisning till bestämmelserna bör alltså föras in i den nya lagen. Med hänsyn till att tillsynsmyndigheten inte bör ha möjlighet att förena förbud med vite (se avsnittet Tillsynsmyndighetens befogenheter) bör någon hänvisning till 32 § andra stycket personuppgiftslagen inte göras i den nya lagen.

Överföring av personuppgifter till tredjeland (33–35 §§)

Personuppgifter som är under behandling får enligt 33 § personuppgiftslagen inte föras över till tredjeland, dvs. en stat som inte ingår i EU eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES; 3 § personuppgiftslagen), om inte det mottagande landet har en adekvat nivå för skyddet av personuppgifter. Från förbudet finns vissa undantag i 34 §, bl.a. för överföring till länder som har anslutit sig till dataskyddskonventionen. Enligt 35 § har regeringen också möjlighet att föreskriva ytterligare undantag från förbudet, bl.a. om det behövs med hänsyn till ett viktigt allmänt intresse.

Förbudet mot överföring till tredjeland som inte har acceptabla skyddsnivåer, och de undantag från förbudet som föreskrivs, bör vara tillämpliga även vid behandling enligt den här föreslagna lagstiftningen. Regeringen bör även ha möjlighet att föreskriva om undantag från förbudet. Hänvisning bör således göras till 33–35 §§ personuppgiftslagen.

Upplysningar till allmänheten, personuppgiftsombudets uppgifter m.m. (38–42 §§)

Automatiserade behandlingar av personuppgifter ska enligt 36 § första stycket personuppgiftslagen anmälas till tillsynsmyndigheten (Datainspektionen). Anmälan behöver dock enligt 3 § personuppgiftsförordningen (1998:1191) inte göras för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning. Någon skyldighet att anmäla de behandlingar som utförs med stöd av den nya lagen finns således inte,

varför någon hänvisning till 36 § första stycket personuppgiftslagen inte behövs.

Den personuppgiftsansvarige kan enligt 36 § andra stycket personuppgiftslagen utse ett personuppgiftsombud. Om ett sådant ombud utses, ska bestämmelserna om ombudets skyldigheter i 38–40 §§ personuppgiftslagen tillämpas. I personuppgiftsombudets skyldigheter ingår bl.a. att se till att behandlingen av personuppgifter sker på ett lagligt sätt och att hjälpa registrerade att få rättelse. Den personuppgiftsansvarige ska anmäla ombudet hos Datainspektionen. Även ett entledigande ska anmälas hos inspektionen. I avsnitt 6.5 föreslås en särskild bestämmelse med skyldighet för polisen att utse personuppgiftsombud och att anmäla till Datainspektionen när ett sådant ombud utses och entledigas. Någon hänvisning till 36 § andra stycket personuppgiftslagen behövs därför inte. Den nya lagen bör dock hänvisa till 38–40 §§ personuppgiftslagen.

Regeringen har enligt 41 § personuppgiftslagen möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll. Detta gäller även vid personuppgiftsbehandling inom polisens brottsbekämpande verksamhet. Denna ordning bör gälla även fortsättningsvis. Den nya lagen bör därför innehålla en hänvisning till 41 §.

Enligt 42 § personuppgiftslagen ska den personuppgiftsansvarige till var och en som begär det lämna upplysningar om de behandlingar av personuppgifter som inte har anmälts till Datainspektionen. Bestämmelsen är tillämplig på de behandlingar som utförs i polisens brottsbekämpande verksamhet men innebär självfallet ingen skyldighet att lämna ut sekretesskyddad information. Det är från integritetsskyddssynpunkt viktigt att den enskilde på ett snabbt och enkelt sätt kan få besked av polisen om vilka behandlingar som utförs i den brottsbekämpande verksamheten även för sådana fall då den behandling som utförs inte omfattas av någon anmälningsskyldighet till Datainspektionen. En hänvisning till 42 § personuppgiftslagen bör därför tas in i den nya lagen.

Tillsynsmyndighetens befogenheter (43–45 §§ och 47 §)

För att kunna säkerställa att personuppgifter behandlas på ett korrekt sätt har Datainspektionen vissa befogenheter gentemot personuppgiftsansvariga. Det är rimligt att Datainspektionen i stort sett har samma befogenheter vid tillsyn över polisens personuppgiftsbehandling i den brottsbekämpande verksamheten som enligt personuppgiftslagen.

Enligt 43 § personuppgiftslagen har Datainspektionen möjlighet att på begäran få tillgång till personuppgifter, upplysningar och dokumentation om behandlingen och säkerheten samt tillträde till lokaler. Paragrafen gäller för polisen och bör vara tillämplig även fortsättningsvis. En hänvisning till paragrafen ska alltså tas in i den nya lagen.

Om Datainspektionen inte efter en begäran enligt 43 § personuppgiftslagen kan få tillräckligt underlag för att konstatera att personuppgiftsbehandlingen är laglig, får myndigheten med stöd av 44 § vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än att lagra dem. Denna bestämmelse gäller för polisens personuppgiftsbehandling och Polisdatautredningen och promemorian föreslår att

den ska gälla även i framtiden. Beträffande andra myndigheters personuppgiftsbehandling har man valt olika lösningar när det gäller Datainspektionens möjlighet att meddela sådana förbud. Någon sådan möjlighet finns exempelvis inte i Tullverkets brottsbekämpande verksamhet och inte heller enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Däremot har Datainspektionen möjlighet att meddela sådana förbud enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar.

När det gäller frågan om Datainspektionen bör ha rätt att förbjuda behandling av personuppgifter i polisens brottsbekämpande verksamhet kan det alltså inledningsvis konstateras att en sådan möjlighet finns enligt gällande rätt. I förhållande till de myndigheter där Datainspektionen saknar sådan möjlighet har polisen en mycket mer omfattande personuppgiftsbehandling som dessutom omfattar flera olika myndigheter. Till detta kan anmärkas att polisen, enligt den nya lagen, kommer att få möjlighet att behandla vissa typer av personuppgifter i större utsträckning än för närvarande. Förslaget lämnar också större utrymme för polisen att fatta beslut om formerna för behandlingen och vilka strukturer den ska ske i. Det sagda talar sammantaget för att Datainspektionen även fortsättningsvis bör kunna förbjuda viss behandling, om det någon gång skulle inträffa att inspektionen inte får tillgång till tillräckligt underlag för att kunna bedöma personuppgiftsbehandlingen. En hänvisning bör därför göras också till 44 §.

En annan fråga är om det bör vara möjligt för Datainspektionen att förena ett sådant förbud med vite. I flera lagstiftningsärenden har en lösning valts som inte ger Datainspektionen någon sådan möjlighet. Detta har motiverats med grundsatsen att regler om vite inte bör tillämpas i förhållandet mellan statliga myndigheter (prop. 2004/05:164 s. 54 och 2006/07:46 s. 105). Eftersom vite inte bör användas mellan statliga myndigheter bör således ett förbud enligt 44 § personuppgiftslagen inte kunna förenas med vite.

En hänvisning bör vidare göras till 45 § första stycket. Där anges att Datainspektionen, om den konstaterar att personuppgifter behandlas felaktigt, ska försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Om det inte går att få till stånd rättelse, eller om saken är brådskande, får Datainspektionen förbjuda behandlingen. Bestämmelsen gäller redan inom polisens brottsbekämpande verksamhet och bör gälla även fortsättningsvis. Däremot bör någon hänvisning till paragrafens andra stycke eller till 46 §, som båda behandlar frågor om vite, inte göras.

Enligt 47 § personuppgiftslagen har Datainspektionen rätt att hos allmän förvaltningsdomstol ansöka om att sådana uppgifter som har behandlats på ett olagligt sätt ska utplånas. Bestämmelsen, som gäller i polisens verksamhet, har sin grund i artikel 28.3 i dataskyddsdirektivet. Där anges att varje nationell tillsynsmyndighet ska ha särskild befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av direktivet har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser. Bestämmelsen bör vara tillämplig vid behandling av uppgifter enligt den nya lagen. En hänvisning till bestämmelsen bör alltså tas in i lagen.

Frågor om tillsyn behandlas även i avsnitt 17.2.

Skadestånd (48 §)

Enligt 48 § personuppgiftslagen ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med den lagen har orsakat. Bestämmelsen gäller vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet.

Det bör finnas en rätt till skadestånd vid skada och kränkning som uppstår när uppgifter behandlas i strid med den nya lagen. En hänvisning till 48 § personuppgiftslagen bör därför tas in i den nya lagen.

I 49 § personuppgiftslagen föreskrivs straffansvar för överträdelser av olika bestämmelser i personuppgiftslagen. Lagrådet har i ett tidigare lagstiftningsärende (prop. 2000/01:33 s. 346) ansett att legalitetsprincipen medför att paragrafen inte kan ges motsvarande tillämpning på bestämmelser som avviker från personuppgiftslagen och som har tagits in i särlagstiftning. Paragrafen kan alltså inte ges en generell tillämpning på de regler som förs in i den nya lagen. Däremot skulle i och för sig en hänvisning kunna tas in i den nya lagen med innebörd att straffbestämmelserna i personuppgiftslagen ska gälla i de delar som personuppgiftslagen ska tillämpas. En sådan ordning kan vid en första anblick förefalla naturlig. Å andra sidan kommer behandlingen av personuppgifter enligt den nya lagen att utföras av personer som är anställda vid statliga myndigheter och som redan omfattas av bestämmelserna om tjänstefel m.m. i brottsbalken. Promemorian ställer sig bakom det uttalande som Polisdatautredningen gör (SOU 2001:92 s. 193) att det inte torde bli aktuellt att tillämpa straffbestämmelsen i personuppgiftslagen mot någon anställd inom polisen (se även prop. 1997/98:97 s. 109). En motsvarande bedömning gjordes vid tillkomsten av lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 55). Även reglerna om disciplinansvar för tjänsteförseelse enligt lagen (1994:260) om offentlig anställning bör enligt regeringens mening vägas in när man bedömer behovet av en regel om straffansvar. Det finns inte skäl att nu göra någon annan bedömning än i tidigare lagstiftningsärenden. Någon hänvisning till bestämmelsen om straffansvar bör därför inte göras i den nya lagen.

Överklagande (51–53 §§)

I 51 § första stycket personuppgiftslagen föreskrivs att Datainspektionens beslut enligt lagen om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol. Förslaget om att Datainspektionen ska kunna meddela förbud enligt 44 § eller 45 § första stycket personuppgiftslagen innebär att en hänvisning också bör göras till 51 § första stycket.

Enligt 51 § andra stycket får Datainspektionen bestämma att dess beslut ska gälla även om det överklagas. Frågan är om denna bestämmelse ska gälla för polisens personuppgiftsbehandling. Det kan finnas skäl som talar både för och emot detta. Systematiska skäl kan tala för att regleringen bör utformas på samma sätt, oavsett vem beslutet gäller.

Emellertid måste verksamhetsskäl anses tala mot införandet av en sådan möjlighet. Vid en samlad bedömning anser regeringen att Datainspektionen inte bör ges möjlighet att meddela interimistiska beslut i här aktuella fall. Hänvisning i den nya lagen bör därför göras endast till 51 § första stycket personuppgiftslagen.

En myndighets beslut om information, rättelse och underrättelse till tredje man om rättelseåtgärder, information om automatiserade beslut och allmänna upplysningar om pågående behandlingar får, enligt 52 § första stycket personuppgiftslagen, överklagas hos allmän förvaltningsdomstol. Andra beslut enligt personuppgiftslagen får enligt 53 § inte överklagas. Prövningstillstånd krävs vid överklagande till kammarrätten. I förarbetena till dessa bestämmelser (prop. 2005/06:173 s. 53) uttalades att det efter införandet av en bestämmelse om överklagande i personuppgiftslagen inte är nödvändigt att ta in några överklagandebestämmelser i särskilda registerförfattningar, som hänvisar till personuppgiftslagen. I konsekvens med detta bör den nya lagen inte innehålla någon särskild bestämmelse om överklagande utan i stället enbart hänvisa till personuppgiftslagens bestämmelser om överklagande.

6.5 Personuppgiftsansvar

Regeringens förslag: Rikspolisstyrelsen och var och en av polismyndigheterna ska vara personuppgiftsansvariga för den behandling av personuppgifter som respektive myndighet utför. Rikspolisstyrelsen ska även vara personuppgiftsansvarig för behandlingen av personuppgifter i polisens verksamhet vid Ekobrottsmyndigheten. Rikspolisstyrelsen och polismyndigheterna ska var och en utse ett eller flera personuppgiftsombud. Detta – liksom entledigande av personuppgiftsombud – ska anmälas till Datainspektionen.

Utredningens förslag: Rikspolisstyrelsen ska ensam vara personuppgiftsansvarig för de centrala registren i polisens verksamhet.

Remissinstanserna har inte haft något att invända mot förslaget.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Ekobrottsmyndigheten* anser att personuppgiftsansvaret för behandling av personuppgifter i polisverksamheten vid myndigheten bör utövas av Ekobrottsmyndigheten. Övriga remissinstanser tillstyrker eller har inte något att invända mot förslaget.

Skälen för regeringens förslag: Enligt 3 § personuppgiftslagen är det den personuppgiftsansvarige som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Personuppgiftsansvaret kan alltså delas mellan flera.

I registerförfattningar är det vanligt att man tydligt pekar ut vem som är ansvarig för den behandling av uppgifter som regleras i respektive författning. I polisdatalagen finns ingen generell bestämmelse om personuppgiftsansvar. I stället anges för respektive register vem som är personuppgiftsansvarig.

I de fall där det rör sig om behandling av uppgifter i större nationella uppgiftssamlingar, bör, liksom tidigare, Rikspolisstyrelsen vara person-

uppgiftsansvarig. Om det å andra sidan handlar om personuppgiftsbehandling inom en polismyndighet, bör ansvaret ligga på denna. Denna ordning för personuppgiftsansvaret bör komma till uttryck i den nya lagen.

Enligt den nya lagen bör som huvudregel gälla att den myndighet som utför själva behandlingen också ska ha personuppgiftsansvaret. När det gäller polisverksamhet vid Ekobrottsmyndigheten bedrivs denna av polispersonal som av Ekobrottskansliet vid Rikspolisstyrelsen ställts till Ekobrottsmyndighetens förfogande. Dessa är således inte anställda vid Ekobrottsmyndigheten. Rikspolisstyrelsen leder den verksamhet vid Ekobrottsmyndigheten som bara får utövas av anställda inom polisen (6 § 7 förordningen [1989:773] med instruktion för Rikspolisstyrelsen). Rikspolisstyrelsen är personuppgiftsansvarig för den personuppgiftsbehandling som sker med stöd av polisdatalagen vid myndigheten (prop. 2002/03:144 s. 17).

Ekobrottsmyndigheten anser att myndigheten bör ha personuppgiftsansvar för behandlingen av personuppgifter i polisens brottsbekämpande verksamhet där. Vad som enligt Ekobrottsmyndigheten talar för en sådan lösning är att polisverksamheten där utgör en del av myndighetens samlade verksamhet. Frågan om myndigheten ska vara personuppgiftsansvarig för personuppgiftsbehandlingen i polisiära datasystem övervägdes i nyssnämnda proposition. Någon förändring som motiverar en annan bedömning beträffande vem som ska vara personuppgiftsansvarig har inte skett. Personuppgiftsansvaret för behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Ekobrottsmyndigheten bör alltså utövas av Rikspolisstyrelsen, vilken bedömning också görs i promemorian. I den mån polispersonal vid Ekobrottsmyndigheten behandlar personuppgifter inom ramen för sådan brottsbekämpande verksamhet som faller utanför den nya lagens tillämpningsområde, exempelvis om de behandlar personuppgifter i åklagarväsendets datasystem, är dessa underkastade den reglering som gäller för sådan verksamhet.

Regleringen i 36 § andra stycket personuppgiftslagen ger myndigheterna valfrihet när det gäller frågan om personuppgiftsombud ska utses eller inte (se avsnitt 6.4.2). Behandlingen av personuppgifter i polisens brottsbekämpande verksamhet rör i stor utsträckning uppgifter som får anses integritetskänsliga, vilket gör det särskilt angeläget med den kontroll som kan utövas av ett personuppgiftsombud. Det är också viktigt att enskilda registrerade enkelt kan vända sig till rätt person hos myndigheten bl.a. i frågor om information om behandlingen och om rättelse av felaktiga uppgifter. Mot den bakgrunden bör det ställas krav på att Rikspolisstyrelsen och polismyndigheterna, som ska ha personuppgiftsansvar enligt den nya lagen, ska utse personuppgiftsombud och anmäla dessa till Datainspektionen. Detta bör framgå direkt av lagen. Det kan anmärkas att regeringen gjorde motsvarande bedömning i propositionen Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (prop. 2006/07:46 s. 98).

6.6 Tillgången till personuppgifter

Regeringens förslag: Tillgången till personuppgifter ska begränsas till vad var och en behöver för att fullgöra sina arbetsuppgifter.

Utredningen föreslår inte någon motsvarande bestämmelse.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inte något att invända mot förslaget. *Datainspektionen* anser att en bestämmelse om tillgång till personuppgifter bör ges en restriktiv tolkning och att huvudregeln bör vara att endast de som har ett direkt behov av uppgifterna bör ha tillgång till dem. Inspektionen anser vidare att den i promemorian föreslagna bestämmelsen är mycket allmänt utformad och att det därför bör införas en regel om att närmare föreskrifter om behörighet och säkerhet ska meddelas av regeringen eller den myndighet som regeringen bestämmer.

Skälen för regeringens förslag: Stora informationsmängder som är samlade så att uppgifter är enkelt sökbara på elektronisk väg medför allmänt sett en risk för intrång i den personliga integriteten. Risken för sådant intrång är särskilt stor om det – som ofta är fallet i brottsbekämpande verksamhet – rör sig om känsliga uppgifter. Vem som har rätt att använda uppgifterna och hur de sprids är omständigheter som påverkar risken för intrång i den personliga integriteten. Det är därför viktigt att det säkerställs att integritetskänsliga uppgifter görs tillgängliga bara för dem som behöver uppgifterna för att fullgöra sitt arbete. Detta bör tydligt framgå av den nya lagen. *Datainspektionen* menar att en bestämmelse om tillgång till personuppgifter bör tolkas restriktivt och att uppgifter i t.ex. en förundersökning bör vara tillgängliga endast för dem som arbetar med denna. En så snäv tolkning av bestämmelsen som Datainspektionen synes förorda skulle lägga hinder i vägen för polisen att utföra sina av statsmakterna påförda uppgifter. I t.ex. en brottsutredning är det många gånger av stor betydelse att polisen kan få information om andra pågående brottsutredningar för att kunna bedöma om det finns några samband mellan utredningarna. Även andra än de som arbetar i en förundersökning bör därför enligt regeringens uppfattning kunna ges möjlighet att få tillgång till uppgifter i undersökningen, om de har ett konkret behov av uppgifterna för att kunna fullgöra sitt arbete.

En bestämmelse om tillgång till personuppgifter bör omfatta både direkt tillgång till automatiserade uppgiftssamlingar och tillgång i allmänhet. Polisen ska således organisera sin verksamhet på ett sådant sätt att obefogad spridning av personuppgifter motverkas.

Modern teknik gör det enklare att organisera verksamheten så att tillgången till uppgifter som behandlas automatiserat begränsas på ett lämpligt sätt. En enskild tjänstemans åtkomst till personuppgifter (behörighet) kan knytas till viss information i stället för till olika register. Därmed kan tillgången till information om en person eller uppgifter knutna till en person begränsas med utgångspunkt från tjänstemannens arbetsuppgifter. De mest känsliga uppgifterna kommer med en sådan ordning att lättare kunna avgränsas och omges av extra integritets- och säkerhetsskydd.

Vidare kommer kunskapen om och kontrollen av varje tjänstemans informationstillgång att öka. På förhand bestämda behörigheter som avgör tillgången till uppgifter kan utarbetas. Behörigheterna kan vidare anpassas till olika befattningshavares behov med hänsyn till tjänstenivå och arbetsuppgifter.

Som nämnts är det en grundläggande regel att personuppgifter inte får behandlas, om det inte behövs för att fullgöra en arbetsuppgift. För att upprätthålla en sådan regel, och motverka att någon användare vidtar otillåtna åtgärder, och därigenom får tillgång till information som denne inte behöver i sitt arbete, krävs det att polisen har säkerhetsarrangemang som gör det möjligt att följa de åtgärder som vidtas med informationen. Denna fråga behandlas närmare i avsnitt 17.1.

Den i promemorian föreslagna bestämmelsen om tillgång till personuppgifter innebär en generell begränsning av åtkomsten till uppgifter för att förhindra att tjänstemän får tillgång till mer information än vad de behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen är, som *Datainspektionen* påpekar, allmänt hållen. Det är emellertid inte lämpligt att i lagform ange detaljerade riktlinjer för hur tillgången till personuppgifter bör avgränsas. I stället är det polisens och övriga berörda myndigheters uppgift att, utifrån respektive myndighets organisation och struktur, säkerställa att åtkomsten till personuppgifter begränsas i enlighet med bestämmelsen. Som Datainspektionen föreslår bör det tydliggöras att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela närmare föreskrifter om tillgången till personuppgifter. En sådan regel bör därför tas in i den nya lagen.

7 Tillåtna ändamål för behandlingen

7.1 Lagens ändamålsreglering

Regeringens förslag: I lagen ska det anges för vilka ändamål behandling av personuppgifter får förekomma. Ändamålen ska delas in i primära ändamål och sekundära ändamål. De primära ändamålen avser behandling av personuppgifter för att tillgodose de behov som finns inom polisen. De sekundära ändamålen avser behandling för olika typer av utlämnande av personuppgifter. I fråga om behandling av personuppgifter för andra ändamål än de primära eller sekundära ändamålen gäller den s.k. finalitetsprincipen i 9 § första stycket d personuppgiftslagen (1998:204).

Utredningens förslag: Personuppgifter ska få behandlas bara om behandlingen är nödvändig för att sådan polisverksamhet som omfattas av lagen ska kunna utföras. Utredningen föreslår också att personuppgifter ska få samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål och att senare behandling inte får ske för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

Promemorians förslag överensstämmer delvis med regeringens. Promemorian föreslår dock en uttömmande reglering av för vilka ändamål personuppgifter får behandlas och finalitetsprincipen föreslås inte vara tillämplig.

Remissinstanserna: Majoriteten av remissinstanserna har inget att anföra mot promemorians förslag. Flera remissinstanser anser dock att förslagets sekundära ändamål är alltför begränsande. *Åklagarmyndigheten* och *Rikspolisstyrelsen* betonar att en uttömmande reglering av ändamålen förutsätter att de sekundära ändamålen får en tillräckligt omfattande räckvidd. *Datainspektionen* anser att förslaget strider mot de centrala dataskyddsprinciper som innebär att personuppgifter endast får samlas in för specifika och legitima ändamål och att personuppgifterna därefter inte får användas på ett sätt som är oförenligt med insamlingsändamålet. Inspektionen anser vidare att det bör ställas krav på att insamlingsändamålet dokumenteras.

Skälen för regeringens förslag

Ändamålsbestämmelserna bör ge utrymme för att bedriva polisarbetet med modern teknik

Den nya lagen ska vara tillämplig i polisens brottsbekämpande verksamhet. Inom ramen för den verksamheten förekommer personuppgiftsbehandling av vitt skilda slag. Dels förekommer mycket sedvanligt kontorsarbete som tidigare inte innebar behandling av personuppgifter, men som gör det med dagens ordbehandlingsteknik. Självklart måste den nya lagen ge polisen samma möjligheter som andra myndigheter att använda modern teknik för att upprätta vanliga dokument, göra löpande noteringar i arbetet m.m. Sådant teknikutnyttjande innefattar inte heller i sig några påtagliga integritetsrisker. Dels förekommer kvalificerad personuppgiftsbehandling, t.ex. i form av uppbyggandet och förandet av stora uppgiftssamlingar som är tillgängliga för flera personer. Sådan behandling ger givetvis upphov till större risker för intrång i den personliga integriteten.

Ett sätt att komma till rätta med integritetsriskerna kan vara att generellt begränsa möjligheterna till behandling av personuppgifter, t.ex. genom att ställa upp snäva ändamålsbestämmelser för alla slag av behandling. Snäva ändamålsbestämmelser kan emellertid allvarligt försämra polisens möjligheter att använda sig av modern kontorsteknik i det brottsbekämpande arbetet. Ett generellt förbud mot behandling av uppgifter som gäller mindre allvarlig brottslighet, t.ex. snatteri, skulle innebära att polisen inte skulle kunna använda sig av sedvanlig ordbehandling i arbetet med att förebygga eller utreda sådan brottslighet. Detta är uppenbarligen inte rimligt. Ändamålsbestämmelserna bör därför utformas så att de ger utrymme för att bedriva polisarbetet på ett effektivt sätt med modern teknik.

De särskilda risker som vissa slag av personuppgiftsbehandling kan ge upphov till bör alltså motverkas på annat sätt. I avsnitt 9 föreslås att bestämmelserna om personuppgiftsbehandling ska göra skillnad mellan *å ena sidan* sådan behandling som avser uppgifter som har gjorts gemensamt tillgängliga och *å andra sidan* annan behandling. Vid behandling av

det förra slaget bör det gälla särskilda bestämmelser som kan minimera de integritetsrisker som mera kvalificerad personuppgiftsbehandling kan ge upphov till.

Personuppgiftslagens regler om ändamål

Bestämmelser om för vilka ändamål uppgifter får behandlas har en central roll i registerförfattningar. Genom ändamålen sätts ramen för vilken behandling som är tillåten. Som *Datainspektionen* framhåller följer det av centrala dataskyddsprinciper att uppgifter endast får samlas in för specifika och legitima ändamål och att insamlade uppgifter inte får behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet. Dessa principer kommer till uttryck bl.a. i artikel 6.1.a i dataskyddsdirektivet och i artikel 3 i dataskyddsrambeslutet. Artikeln i dataskyddsdirektivet har genomförts i svensk rätt genom 9 § första stycket c och d personuppgiftslagen.

I fråga om efterföljande behandling sägs i 9 § andra stycket personuppgiftslagen att en behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte ska anses som oförenlig med de ändamål för vilka uppgifterna samlades in. I de fall där en tilltänkt behandling inte direkt omfattas av de ursprungliga ändamålen måste det i princip prövas om ändamålet med den senare behandlingen är oförenlig med de ursprungliga ändamålen. Detta följer av den s.k. finalitetsprincipen, som uttrycks i 9 § första stycket d personuppgiftslagen.

Datalagskommittén uttalar i betänkandet Integritet – Offentlighet – Informationsteknik (SOU 1997:39 s. 351) att vad som är oförenligt med de ursprungliga ändamålen får bestämmas genom praxis och de mer preciserade regler som regeringen och Datainspektionen kan utfärda.

Den nya lagens ändamålsreglering och finalitetsprincipen

Utgångspunkten i den nya lagen är att personuppgifter får behandlas enbart för vissa berättigade, angivna ändamål. Därmed kan användningen och spridningen av uppgifterna begränsas. Frågan är då hur ändamålsregleringen bör utformas.

Det är vanligt att man i registerförfattningar delar upp ändamålen i primära och sekundära. De *primära ändamålen* är utformade för att tillgodose den behandling som behövs i de berörda myndigheternas egen verksamhet. *Sekundära ändamål* reglerar i vilken utsträckning uppgifter, som samlats in för något primärt ändamål, får behandlas för att lämnas ut till enskilda eller till andra myndigheter i syfte att tillgodose deras behov. För polisens del kan det vara fråga om att uppgifter i den brottsbekämpande verksamheten behöver användas i annan polisverksamhet eller att uppgifterna behövs i brottsbekämpande verksamhet som någon annan myndighet bedriver.

Det finns flera olika möjligheter att utforma ändamålsregleringen i registerförfattningar. Det går dock att urskilja två principiellt olika sätt. Det ena är att ange samtliga ändamål för vilka behandling får ske, både primära och sekundära. Det andra är att ange de primära ändamålen uttömmande medan de sekundära ändamålen – i den mån sådana anges –

kompletteras med en möjlighet att vidarebehandla uppgifter även för ändamål som inte är oförenliga med insamlingsändamålet. Möjligheten till vidarebehandling får således avgöras med tillämpning av finalitetsprincipen. I flertalet registerlagar, däribland polisdatalagen, är ändamålsbestämmelserna utformade enligt det senare alternativet. Även Polisdatautredningen föreslår en sådan lösning. Promemorian förordar däremot att ändamålen anges uttömmande enligt det förra alternativet. Den lösningen har också valts i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

En utgångspunkt bör vara att tillåtna ändamål anges så tydligt och fullständigt som möjligt. Insamlingsändamålen, dvs. de primära ändamålen, bör anges uttömmande. En svårare fråga är om även de sekundära ändamålen, som syftar till att beskriva för vilka ändamål uppgifter får lämnas ut, bör anges uttömmande. Det kan finnas fördelar med en sådan reglering. Lagstiftaren kan sägas en gång för alla ha bestämt i vilken utsträckning uppgifter ska få behandlas för att spridas till andra. Under förutsättning att ändamålen är tydligt avgränsade står det genom en sådan reglering klart både för tillämpare och andra vilken personuppgiftsbehandling som får förekomma med stöd av den aktuella lagen. I förarbetena till flera registerlagar har man dock gjort bedömningen att det inte är möjligt att i en lag om personuppgiftsbehandling på ett tillräckligt preciserat sätt ange alla de situationer där utlämnande av uppgifter kan komma att aktualiseras.

Att bedöma nuvarande och förutse framtida behov av att kunna utlämna uppgifter är särskilt svårt i en sådan varierad och omfattande verksamhet som polisens brottsbekämpande verksamhet. Flera remissinstanser har också pekat på att promemorians förslag avseende sekundära ändamål är för begränsande. Även *Datainspektionen* kritiserar promemorians förslag för att det inte innehåller någon hänvisning till finalitetsprincipen.

Vid en samlad bedömning anser regeringen att finalitetsprincipen bör komplettera lagens ändamål på samma sätt som i många andra registerlagar. I lagen bör de sekundära ändamålen uttryckas så preciserat och fullständigt som möjligt. För andra ändamål än de i lagen angivna sekundära ändamålen bör utlämnande tillåtas enbart under förutsättning att det inte kan anses oförenligt med insamlingsändamålet att lämna ut uppgifterna, dvs. med tillämpning av finalitetsprincipen. Det föreslås således att en hänvisning görs till 9 § första stycket d personuppgiftslagen (avsnitt 6.4.2).

Datainspektionen är vidare kritisk till att det saknas krav på att ett närmare preciserat insamlingsändamål anges och dokumenteras. Inspektionen menar att om inte finalitetsprincipen gäller och det inte ställs krav på specifika ändamål tillåts uppgifter flöda fritt inom polisens brottsbekämpande verksamhet.

Inledningsvis kan konstateras att Datainspektionens uppfattning att polisen vid insamling av uppgifter måste ha ett närmare preciserat ändamål för insamlingen, t.ex. att utreda ett visst brott, har fog för sig. Därför föreslår regeringen, i motsats till promemorian, att den nya lagen hänvisar till 9 § första stycket c personuppgiftslagen (se avsnitt 6.4.2). Skyldigheten att ha ett preciserat ändamål för insamlingen kan visserligen sägas följa redan av de materiella bestämmelser som styr polisens verk-

samhet. Detsamma gäller för den fortsatta behandlingen. Varje åtgärd (inklusive vidarebehandling) som polisen vidtar med insamlade uppgifter, måste naturligtvis ske för ett närmare preciserat ändamål (när det gäller lagringen, se avsnitt 14.1). I den nya lagen föreslås vidare bestämmelser som ställer krav på att det av uppgifter som har gjorts gemensamt tillgängliga ska framgå för vilket närmare ändamål en uppgift behandlas, se avsnitt 10. Något annat krav på dokumentation kan inte anses nödvändigt. Något sådant krav finns inte heller i andra registerlagar.

Hänvisningen till 9 § första stycket c personuppgiftslagen innebär att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Enligt finalitetsprincipen får de insamlade uppgifterna sedan inte behandlas för ändamål som är oförenliga med det ursprungliga ändamålet.

En av polisens av statsmakterna fastlagda övergripande uppgifter är att utreda brott och bekämpa brottslig verksamhet. Har personuppgifter samlats in för att utreda ett visst brott kan det generellt sett – mot bakgrund av polisens övergripande uppgift – inte anses vara oförenligt med det ursprungliga ändamålet att behandla samma uppgifter för att utreda annat brott eller bekämpa brottslig verksamhet. I vissa undantagsfall har lagstiftaren dock bedömt att behandling för sådana nya ändamål inte bör vara tillåten. Uttrycklig reglering om detta har då införts. Sådan reglering finns i bl.a. 27 kap. 23 a § rättegångsbalken och 12 § lagen (2007:978) om hemlig rumsavlyssning, som begränsar användningen av s.k. överskottsinformation från hemliga tvångsmedel till enbart de fall som direkt anges i paragrafen. Vidare kan det – när svenska myndigheter mottar uppgifter från andra stater – finnas villkor som på grund av en internationell överenskommelse är bindande för de svenska myndigheterna och som begränsar möjligheterna att använda uppgifterna eller bevisningen. I bl.a. 3 § lagen (2000:343) om internationellt polisiärt samarbete och 5 kap. 1 § lagen (2000:562) om internationell rättslig hjälp finns bestämmelser som innebär att svenska myndigheter ska följa sådana villkor oavsett vad som är föreskrivet i lag eller annan författning.

En grundtanke med förslaget är således att det inom polisen bör vara tillåtet att använda sig av uppgifter som samlats in för ett visst brottsbekämpande ändamål för ett annat sådant ändamål, om polisen har behov av detta och det är tillåtet enligt den reglering som gäller för polisens verksamhet. Under sistnämnda förutsättning bör vidarebehandling också få ske om det behövs för brottsbekämpande ändamål hos andra myndigheter eller för vissa andra sekundära ändamål som kan förutses och som anses förenliga med finalitetsprincipen. Genom att ange de primära ändamålen och nämnda sekundära ändamål i lagen görs ställningstagandet att vidarebehandling för dessa ändamål är förenlig med finalitetsprincipen. För att en uppgift ska kunna vidarebehandlas för något annat än de i lagen angivna ändamålen måste det däremot i det enskilda fallet göras en bedömning att det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in. I syfte att åstadkomma ett fullgott integritetsskydd kompletteras den föreslagna ändamålsregleringen vidare med andra bestämmelser som sätter gränser för behandlingen, t.ex. bestämmelser om tillgång till uppgifter och om gallring. Det bör vidare framhållas att ett utlämnande alltid måste vara förenligt med offentlig-

hets- och sekretesslagen (2009:400), vilket ger ett grundläggande integritetsskydd.

I avsnitten 7.2–7.4 diskuteras vilka de *primära* ändamålen för behandlingen av personuppgifter i polisens brottsbekämpande verksamhet bör vara. I avsnitt 7.6 behandlas de *sekundära* ändamålen.

Bestämmelserna om ändamål för behandling av personuppgifter bör inte få hindra rationella rutiner för diarieföring och ärendehantering. Det har föranlett särskilda överväganden som redovisas i avsnitt 7.5.

I 8 § första stycket personuppgiftslagen, som föreslås vara tillämplig på behandlingen av personuppgifter enligt den nya lagen, finns en erinran om att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Bestämmelser i grundlag tar över bestämmelser i vanlig lag. Tryckfrihetsförordningens bestämmelser har därför företräde framför bestämmelserna i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Behandling av personuppgifter kommer därmed alltid att vara tillåten för att uppfylla de krav som offentlighetsprincipen ställer.

7.2 Förebygga, förhindra eller upptäcka brottslig verksamhet

Regeringens förslag: Personuppgifter ska få behandlas i polisens brottsbekämpande verksamhet, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Utredningen föreslår att bestämmelserna om kriminalunderrättelseverksamhet och kriminalunderrättelseregister ersätts med bestämmelser om behandling av uppgifter om andra personer än sådana som är misstänkta för brott. Enligt utredningen ska sådana uppgifter få behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Utredningen föreslår vidare att det under vissa förutsättningar ska vara tillåtet att behandla uppgifter, om det är nödvändigt för att underlätta övervakning av vissa grovt kriminellt belastade personer och personer som kan antas vara farliga.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller inte invänt mot förslaget att utmönstra begreppen kriminalunderrättelseverksamhet och kriminalunderrättelseregister. *Datainspektionen* har dock ansett att nuvarande regler är väl avvägda. Majoriteten av remissinstanserna har ställt sig positiv till förslaget om att införa särskilda bestämmelser om behandling av uppgifter om personer som inte är misstänkta för brott.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna godtar promemorians förslag eller har inget att invända mot det. *Datainspektionen* anser att det finns ett stort behov av att modernisera lagstiftningen avseende kriminalunderrättelseverksamhet men tycker att den föreslagna

regleringen är för generellt utformad. Den innebär enligt inspektionen att verksamheter med helt olika förutsättningar, behov och risker kommer att styras av samma reglering. Inspektionen efterlyser en analys av hur de olika brottsförebyggande verksamheterna påverkas av regleringen och menar att det inte utan en sådan analys går att göra en proportionalitetsbedömning av det slag som förutsätts enligt bl.a. Europakonventionen. För behandling av uppgifter som inte har gjorts gemensamt tillgängliga anser inspektionen att den föreslagna regleringen helt saknar begränsningar.

Kustbevakningen anser att rekvisitet ”förebygga” brottslig verksamhet inte bör omfattas av ändamålen. *Tullverket* delar däremot promemorians uppfattning att ”förebygga” bör inkluderas bland ändamålen.

Skälen för regeringens förslag

Begreppet kriminalunderrättelseverksamhet bör inte användas

Inledningsvis måste ställning tas till i vilken utsträckning personuppgifter bör få behandlas inom ramen för brottsbekämpande verksamhet som inte avser utredning eller beivrande av ett bestämt brott. Hittills har sådan personuppgiftsbehandling skett inom ramen för polisdatalagens (1998:622) bestämmelser om kriminalunderrättelseverksamhet och kriminalunderrättelseregister. Å ena sidan måste polisen, för att kunna bedriva ett framgångsrikt brottsförebyggande arbete, få behandla uppgifter om personer som inte är misstänkta för något konkret brott men väl för att medverka i pågående eller planerad brottslig verksamhet. Å andra sidan skulle en möjlighet för polisen att utan någon närmare begränsning behandla personuppgifter som inte har samband med något konkret brott öppna vägen för en omfattande behandling av personuppgifter med betydande risker för intrång i den personliga integriteten.

Underrättelseverksamhet definieras i 3 § första stycket polisdatalagen som polisverksamhet som består i att samla in, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken. Motsvarande definition finns i 2 § första stycket lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och i 2 § första stycket i den numera upphävda lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. I polisdatalagen tar begreppet sikte på all underrättelseverksamhet som bedrivs hos polisen. För sådan underrättelseverksamhet som bedrivs av annan än Säkerhetspolisen används i sistnämnda lag begreppet kriminalunderrättelseverksamhet.

Som tidigare nämnts tillåter polisdatalagen inte att personuppgifter behandlas i kriminalunderrättelseverksamhet annat än under vissa förutsättningar som anknyter till hur polisen ska bedriva sådan verksamhet. En förutsättning är att en särskild undersökning har inletts (14 § första stycket polisdatalagen). Med begreppet särskild undersökning avses en undersökning i kriminalunderrättelseverksamhet som innebär insamling, bearbetning och analys av uppgifter i syfte att ge underlag för beslut om förundersökning eller om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Har en särskild undersökning inletts, får personupp-

gifter behandlas, om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas.

Vidare får personuppgifter behandlas i kriminalunderrättelseregister för att ge underlag för de nyss nämnda särskilda undersökningarna eller underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet (17 § polisdatalagen). Sådana register får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet utövats eller kan komma att utövas och de som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva den brottsliga verksamheten (19 § polisdatalagen). Vissa indirekta personuppgifter, t.ex. om transportmedel, får också behandlas i registren.

Som både Polisdatautredningen och promemorian framhåller är polisdatalagens systematik med reglering av kriminalunderrättelseverksamhet och kriminalunderrättelseregister, ägnad att ge upphov till tillämpningssvårigheter. Definitionen av kriminalunderrättelseverksamhet täcker även sådan behandling av personuppgifter som rimligen inte är så känslig att den behöver regleras särskilt. Den omfattar, utöver det arbete som sker inom ramen för särskilda undersökningar, även polisens dagliga löpande arbete med att hantera information som på olika sätt kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet. Eftersom polisdatalagen utgår från att all behandling av uppgifter för de nu aktuella ändamålen ska ske inom ramen för särskilda undersökningar eller kriminalunderrättelseregister, har lagen kommit att försvåra polisens arbete med att verka problemorienterat och brottsförebyggande. Samtidigt har regleringen skapat oklarheter beträffande flera andra register som polisen för. Polisdatautredningen och promemorian pekar på att det kan ifrågasättas om inte behandlingen av personuppgifter i vissa existerande polisregister till viss del skulle kunna tolkas som kriminalunderrättelseverksamhet i polisdatalagens mening. Behandlingen skulle därmed inte vara tillåten annat än under de särskilda förutsättningar som gäller för behandling av uppgifter i kriminalunderrättelseverksamhet.

Av dessa skäl bör man, som både Polisdatautredningen och promemorian föreslår, inte använda begreppet kriminalunderrättelseverksamhet i den nya lagen.

Ändamålen bör vara att förebygga, förhindra eller upptäcka brottslig verksamhet

Som nyss har nämnts användes begreppet underrättelseverksamhet i den numera upphävda lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Begreppet fördes dock inte över till den nuvarande lagen i samma ämne. Den lagen innehåller i stället bestämmelser om behandling av personuppgifter för ändamålen att förhindra eller upptäcka brottslig verksamhet. Samma lösning bör väljas för polisens del. I förtydligande syfte bör bestämmelsen även innehålla ordet förebygga. *Tullverket* uttalar sitt stöd för detta tillägg. Av den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör alltså framgå att personuppgifter får behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet. Därmed kom-

mer bestämmelsen att ge utrymme för personuppgiftsbehandling inom all egentlig brottsbekämpande verksamhet inom polisen som inte direkt kan knytas till en brottsutredning, däribland behandling i polisens underrättelseverksamhet. Både behandling av mera rutinmässig karaktär, t.ex. ordbehandling, och behandling av mera kvalificerat slag kommer att omfattas av bestämmelsen.

Kustbevakningen anser att det strider mot en väl etablerad rättslig terminologi att låta ”förebygga brottslig verksamhet” omfattas av beskrivningen av kriminalunderrättelseverksamhet och att det skapar en påtaglig otydlighet i förhållande till den ordningshållande verksamheten. Som nyss nämnts är avsikten inte att det nu behandlade ändamålet enbart ska omfatta vad som traditionellt sett har betecknats som kriminalunderrättelseverksamhet, utan vara något vidare. Frågan om eventuella gränsdragningsproblem i förhållande till annan polisiär verksamhet behandlas i avsnitt 6.3.

Vilka begränsningar bör gälla för behandlingen?

Regleringen i polisdatalagen av behandling av personuppgifter i kriminalunderrättelseverksamhet har som tidigare nämnts lett till tillämpningsproblem. Regleringen av formen för behandlingen i särskilda undersökningar och kriminalunderrättelseregister har dessutom ansetts för begränsande för att tillgodose polisens behov av att bedriva en modern och effektiv brottsbekämpande verksamhet.

Frågan är om det är lämpligt att i en lag som reglerar personuppgiftsbehandling reglera i vilken form en myndighet ska bedriva sitt arbete. Så bör vara fallet endast om det är nödvändigt för regleringen av själva personuppgiftsbehandlingen. Avsikten med en sådan lag bör inte vara att detaljreglera en myndighets verksamhet. En detaljreglering försvårar också myndighetens möjlighet att anpassa sina arbetsformer till förändrade krav och förväntningar. Från integritetsskyddssynpunkt är det, som både Polisdatautredningen och promemorian har funnit, inte nödvändigt att i den nya lagen införa bestämmelser om arbete i projektform motsvarande de bestämmelser som finns om s.k. särskilda undersökningar. Från integritetsskyddssynpunkt finns det inte heller skäl att införa särskilda bestämmelser om kriminalunderrättelseregister.

Som nämns i avsnitt 7.1 och utvecklas närmare i avsnitt 9, bör olika regler gälla för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga och behandling av personuppgifter som endast ett fåtal tjänstemän har tillgång till. Skillnad bör göras mellan behandling av personuppgifter som sker i större respektive mindre projekt. Utgångspunkterna som bör gälla för gränsdragningen mellan större och mindre projekt redovisas i avsnitt 9.1. Som polisen har påpekat kommer den allra största delen av dess personuppgiftsbehandling att omfattas av reglerna för behandling av gemensamt tillgängliga uppgifter. För denna behandling bör ett flertal begränsande bestämmelser gälla som syftar till att åstadkomma en väl avvägd balans mellan verksamhetsintressen och integritetsskyddsintressen (jfr bl.a. avsnitt 9–11 och 14). För övrig behandling som behövs för att förebygga, förhindra eller upptäcka brottslig

verksamhet är det däremot tillräckligt från integritetsskyddssynpunkt att grundläggande dataskyddsbestämmelser gäller.

Regeringen delar således inte *Datainspektionens* uppfattning att den reglering som föreslås i promemorian inte begränsar polisens möjligheter att behandla personuppgifter i tillräckligt hög grad. Det finns andra bestämmelser som styr hur polisen ska bedriva sin verksamhet. Den polisman som – för att ta ett av inspektionens exempel – i den egna datorn samlar uppgifter om allmänt misskötsamma ungdomar utan att ha ett bestämt brottsbekämpande syfte med behandlingen gör sig sannolikt skyldig till en tjänsteförseelse som kan beivras disciplinärt. Det bör dock betonas att det i det brottsförebyggande arbetet kan finnas sakliga skäl för exempelvis närpolisen att anteckna uppgifter om ungdomar i närområdet som bedöms befinna sig i riskzonen för att inleda en brottslig bana. Bedömningen kan t.ex. grunda sig på information från skola, föräldrar eller socialtjänst. Sådana noteringar har polisen alltid gjort. Bara för att anteckningar numera sker med hjälp av en dator bör behandlingen inte anses otillåten.

Vilken verksamhet omfattas av ändamålen?

Behandling av personuppgifter i brottsbekämpande verksamhet där det inte finns någon misstanke om ett konkret brott är särskilt känslig från integritetssynpunkt. Som *Datainspektionen* framhåller ingår i polisens uppgifter verksamheter av skilda slag där behovet av att behandla integritetskänsliga uppgifter varierar. Datainspektionen efterfrågar en redogörelse för de skilda behov och förutsättningar som olika brottsförebyggande verksamheter medför och en analys av hur den föreslagna regleringen kan komma att påverka de olika verksamheterna. Nedan följer en beskrivning av den verksamhet som är tänkt att omfattas av ändamålen förebygga, förhindra eller upptäcka brottslig verksamhet och hur polisen organiserar detta arbete. Redogörelsen är inte uttömmande. Den illustrerar svårigheten att dra en klar gräns mellan de olika verksamheter som inryms i ändamålen.

Den verksamhet som framför allt avses med de aktuella ändamålen är den som normalt kallas underrättelseverksamhet. Arbetet består främst i att samla in, bearbeta och analysera information och bedrivs numera enligt polisens underrättelsemodell (PUM). Detta är en modell för ledning och styrning av planlagd operativ polisverksamhet där beslut om inriktning, prioritering och genomförande baseras på underrättelser och annan relevant kunskap. Enligt modellen ska underrättelseverksamhet bedrivas på lokal, regional och central nivå. Polisen beskriver den nuvarande verksamheten på följande sätt.

Den *lokala* kriminalunderrättelsetjänsten finns på samtliga polismyndigheter och utgör basen i underrättelseverksamheten. Dels arbetar den med de problem som är viktiga för den egna polismyndigheten, dels medverkar den i kriminalunderrättelseverksamhet som har regional, nationell och internationell bäring.

På *regional* nivå finns för närvarande sju samverkansområden. För att knyta samman den lokala och nationella kriminalunderrättelseverksamheten finns det, utifrån vad som överenskommits mellan polismyndighe-

terna i respektive samverkansområde, en regional nivå för kriminalunderrättelsetjänsten. Den regionala kriminalunderrättelsetjänsten ska vara samverkans- och samordningsfunktion för kriminalunderrättelsetjänsten inom respektive samverkansområde samt mellan dessa områden. Den ska också utgöra en länk till Rikskriminalpolisens nationella kriminalunderrättelsetjänst. Polismyndigheterna i Västra Götaland, Stockholms län och Skåne har under några år i projektform drivit regionala underrättelsecentrum där både brottsbekämpande och andra myndigheter ingår. Exempel på det senare är Kronofogdemyndigheten och Skatteverkets fiskala del. Dessa underrättelsecentrum har under våren 2009 permanentats och fem nya har inrättats.

Den *nationella* kriminalunderrättelseverksamheten bedrivs vid Rikskriminalpolisen och är huvudsakligen inriktad mot grova brott och grov organiserad brottslighet på nationell och internationell nivå. Rikskriminalpolisen ska inom vissa prioriterade områden bedriva långsiktiga operativa underrättelseprojekt samt strategiska projekt. Underrättelsesektionen vid Rikskriminalpolisen utgör således ett nationellt underrättelsecentrum. Av intresse här är Rikskriminalpolisens del i samordningen av den nationella satsningen mot grov organiserad brottslighet i Samverkansrådet och i det Operativa rådet.

I departementspromemorian Nationell mobilisering mot den grova organiserade brottsligheten – överväganden och förslag (Ds 2008:38) lämnas ett flertal förslag, bl.a. på hur organisationen av polisens underrättelseverksamhet kan utvecklas. Med anledning av promemorian gav regeringen i juli 2008 Rikspolisstyrelsen i uppdrag att vidta åtgärder för att säkerställa en effektiv och uthållig verksamhet för bekämpning av den grova organiserade brottsligheten (dnr Ju2008/5776/PO). I slutredovisningen av uppdraget framgår bl.a. att polisen har vidtagit följande åtgärder (dnr Ju2009/5516/PO).

Förutom att det har inrättats ytterligare fem regionala underrättelsecentrum har det tidigare Operativa rådet vid Rikskriminalpolisen delats upp i ett samverkansråd och ett nytt operativt råd. Råden består av representanter för polisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen, Skatteverket, Kriminalvården och Kronofogdemyndigheten. Samverkansrådet har som huvuduppgift att besluta om en gemensam nationell inriktning för insatserna mot grov organiserad brottslighet. Operativa rådet har till uppgift att fatta beslut om operativa insatser mot grov organiserad brottslighet som förutsätter medverkan från olika myndigheter. Inom polisen har det vidare inrättats en nationell strategisk ledningsgrupp för att fastställa en polisiär gemensam strategisk inriktning för arbetet mot den grova organiserade brottsligheten. I denna ingår, utöver representanter för Rikspolisstyrelsen, länspolismästarna vid de polismyndigheter som har regionala underrättelsecentrum.

Inhämtning av underrättelseinformation sker på flera olika sätt. I stor utsträckning sker det genom öppna källor, men en inte obetydlig del av inhämtningen sker genom informatörer eller andra hemliga källor. En viktig del i underrättelsetjänsten utgörs av s.k. inre spaning, dvs. sökande efter information som redan finns tillgänglig inom polisen. I detta arbete ingår bl.a. sökning i register. Genom samarbete med andra myndigheter, företag och andra inhämtas också information. Även internationellt samarbete spelar en stor roll. Det gäller såväl organiserat polisiärt samarbete i

multilaterala eller bilaterala former som mera informellt sådant samarbete. Genom kontakter med bl.a. myndigheter i andra länder får polisen också information inom ramen för underrättelseverksamhet.

Utifrån hur polisen organiserat sin underrättelseverksamhet kan, något förenklat, polisens underrättelsemodell beskrivas på följande sätt. Kriminalunderrättelsetjänsten samlar in information, både på egen hand och genom att ta emot information som samlas in av andra enheter inom polisen. Informationen bearbetas och analyseras och leder fram till underrättelser. Underrättelserna delges den operativa ledningen som med underrättelserna som underlag fattar beslut om prioriteringar och adekvata brottsförebyggande aktiviteter (planlagd linjeverksamhet och planlagd insats). Kriminalunderrättelsetjänsten avgör vilken underrättelseinformation som ska delges de tjänstemän inom polisen som bedriver brottsbekämpande verksamhet. Vilka uppgifter som delges styrs av de prioriteringar som den operativa ledningen har beslutat och av överväganden som tar sikte på integritetsskyddsintressen.

Den aktuella modellen bygger således på ett flöde av information. Alla anställda inom polisen har ett ansvar för att inhämta information. Om en polisman gör iakttagelser som bedöms ha samband med misstänkt brottslig verksamhet ska informationen samlas in, dokumenteras och vidarebefordras till kriminalunderrättelsetjänsten. Informationsinhämtningen ska koncentreras till prioriterade problem. Kriminalunderrättelsetjänsten ansvarar för att annan personal inom polisen ständigt hålls informerad om inom vilka områden uppgifter främst efterfrågas, dvs. vilka de prioriterade underrättelsebehoven är. Polismän i yttre tjänst ska känna till vilka företeelser eller personer som det är särskilt viktigt att vara uppmärksam på. Den information som delges polismän i yttre tjänst kan vara av mer generellt slag eller avse vissa utpekade personer, t.ex. några som misstänks för delaktighet i brottslig verksamhet. Merparten av underrättelseinformationen stannar inom kriminalunderrättelsetjänsten. Det är i huvudsak slutsatserna av analys och bearbetning som förmedlas till andra delar av polisen.

Den beskrivna modellen förutsätter att uppgifter som inte rör misstanke om något konkret brott men väl misstanke om brottslig verksamhet, får behandlas automatiserat. Sådan behandling behövs bl.a. för insamling, dokumentation, förmedling till kriminalunderrättelsetjänsten, bearbetning och analys samt för vidareförmedling av relevant underrättelseinformation.

Personuppgiftsbehandling behövs enligt regeringens mening både i verksamhet vid särskilda underrättelseenheter och i den operativa verksamheten som i polisens underrättelsemodell beskrivs som planlagd linjeverksamhet och planlagd insats. Behovet av att behandla uppgifter och omfattningen av behandlingen skiljer sig dock åt.

Brottsförebyggande arbete bedrivs ofta i projektform på lokal, regional och nationell nivå. Storleken på projekten varierar liksom varaktigheten. Projekt är inte sällan myndighetsöverskridande. Den verksamhet som bedrivs kan sägas vara underrättelsestyrd eftersom projekten ofta startas för att komma till rätta med någon typ av brottslighet som är prioriterad. Syftet med ett projekt kan bl.a. vara att ta fram modeller och metoder i arbetet med att förebygga brott inom ett visst område. Många projekt bedrivs utan att någon personuppgiftsbehandling är nödvändig. Andra

projekt förutsätter sådan behandling. Som exempel på det senare kan nämnas projekt som syftar till att komma till rätta med ungdomsbrottsligheten i ett visst område. Sådana projekt bedrivs för närvarande vanligtvis inom ramen för en särskild undersökning.

Sammanfattningsvis har polisen ett stort behov av att kunna behandla personuppgifter även i sådan brottsbekämpande verksamhet som inte avser utredning eller beivrande av ett bestämt brott. En grundläggande förutsättning bör vara att behandlingen ska behövas för att förebygga, förhindra eller upptäcka brottslig verksamhet.

I sammanhanget är det viktigt att framhålla att underrättelseverksamhet i traditionell mening även fortsättningsvis kommer att bedrivas vid särskilda enheter med särskilt utbildade tjänstemän. Det är också en naturlig del i underrättelsearbete att begränsa antalet tjänstemän som får del av viss information, t.ex. när man kartlägger organiserad eller annan allvarlig brottslighet. Det innebär allmänt sett en risk att sprida uppgifter av underrättelsekaraktär till en vidare krets. Den faktiska tillgången till uppgifter kommer alltså att variera beroende på hur känsliga uppgifterna är och behovet av tillgång till uppgifterna. Utvecklingen inom polisen går mot att öka kompetensen hos den personal som analyserar och bearbetar särskilt känslig information. Vidare utvecklas fortlöpande olika modeller för att värdera information.

7.3 Utreda och beivra brott

Regeringens förslag: Personuppgifter ska få behandlas i polisens brottsbekämpande verksamhet, om det behövs för att utreda eller beivra brott.

Utredningens förslag: Personuppgifter ska alltid få behandlas, om det är nödvändigt för att bedriva utredning i fråga om brott som hör under allmänt åtal.

Remissinstanserna har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Datainspektionen* anser att den föreslagna ändamålsbestämmelsen har en låg grad av konkretion och att det torde krävas att det anges för vilket närmare slag av brott som behandling sker.

Skälen för regeringens förslag: Att utreda och beivra brott är en central uppgift för polisen. Arbetet sker framför allt inom ramen för förundersökningar enligt 23 kap. rättegångsbalken. Exempel på sådant arbete är spaning, förhör, informationsbearbetning och olika former av beslutsfattande, bl.a. om tvångsmedelsanvändning. Till uppgiften att utreda och beivra brott hör också sådant arbete som sker inom ramen för förenklade förfaranden vilka kan mynna ut i utfärdande av strafföreläggande eller föreläggande av ordningsbot. Hit hör även utredningar som polisen gör enligt reglerna i 23 kap. rättegångsbalken med stöd av bestämmelser i

särskilda författningar, t.ex. utredningar enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, 9 § lagen (1988:688) om besöksförbud, 8 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang, 16 § lagen (1957:668) om utlämning för brott, 10 § lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge och 4 kap. 3 § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. I arbetet med att utreda och beivra brott innefattas också sådan behandling av personuppgifter som sker med stöd av 23 kap. 3 och 8 §§ rättegångsbalken innan förundersökning har inletts samt andra åtgärder som vidtas i syfte att samla in underlag för beslut om huruvida förundersökning ska inledas eller inte, s.k. förutredning. Till uppgiften att beivra brott hör främst föreläggande av ordningsbot men också biträde åt åklagare bl.a. i ärenden om undanröjande av ordningsbot eller straffföreläggande, ändring av påföljd och utlämning för verkställighet av straff.

Arbetet med att utreda och beivra brott skiljer sig åt från arbetet med att förebygga, förhindra eller upptäcka brottslig verksamhet. I det förra fallet utförs arbetet med anledning av att ett konkret brott har eller misstänks ha begåtts, medan arbetet i det senare fallet utförs med anledning av misstankar om pågående brottslig verksamhet som inte kan konkretiseras eller allmänna misstankar om framtida brott. Det är självklart att personuppgifter måste få behandlas även inom ramen för arbetet med att utreda och beivra brott. En förutsättning är givetvis att behandlingen behövs för ändamålet.

Datainspektionen anser att de i promemorian föreslagna ändamålen är för vaga och torde rymma de flesta uppgifter som skulle kunna samlas in. Som nämns i avsnitt 7.2 regleras emellertid polisens verksamhet av en mängd olika bestämmelser som gäller utöver regleringen av personuppgiftsbehandling. De bestämmelser som styr polisens verksamhet att utreda och beivra brott torde regelmässigt utesluta varje form av åtgärd i fall där koppling saknas till en specifik brottsmisstanke. Här kan bl.a. erinras om skyldigheten att fatta ett formellt beslut om att inleda förundersökning och att dokumentera detta enligt 1 a § förundersökningskungörelsen (1947:948). Motsvarande krav gäller när en förundersökning utvidgas till att omfatta nya brott. Mot denna bakgrund kan det inte anses nödvändigt med några ytterligare begränsningar i fråga om vilka uppgifter som ska få behandlas för ändamålen utreda eller beivra brott. På samma sätt som föreslås i fråga om personuppgiftsbehandling för att förebygga, förhindra eller upptäcka brottslig verksamhet bör endast de grundläggande bestämmelserna i den nya lagen vara tillämpliga så länge uppgifterna inte görs gemensamt tillgängliga.

7.4 Internationellt samarbete

Regeringens förslag: Personuppgifter ska få behandlas i polisens brottsbekämpande verksamhet, om detta krävs för att fullgöra ett internationellt åtagande.

Utredningen föreslår inte några särskilda ändamålsbestämmelser för det internationella samarbetet.

Remissinstanserna har inte yttrat sig i saken.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Rikspolisstyrelsen* påpekar att samarbetet inom Interpol sker på grundval av överenskommelser mellan medlemsstaterna och att det är tveksamt om det omfattas av promemorians definition av ”internationella åtaganden”. Styrelsen anser därför att Interpol-samarbetet bör kommenteras särskilt under den fortsatta beredningen. Styrelsen anser vidare att det bör klargöras att trafikövervakning inom ramen för EU-samarbetet omfattas av den föreslagna lagen.

Skälen för regeringens förslag: Med ökad internationalisering och större rörlighet för såväl personer och kapital som varor och tjänster följer större krav på polisiärt samarbete över gränserna, särskilt om allvarlig och organiserad brottslighet ska kunna bekämpas effektivt. Det polisiära samarbetet regleras i stor utsträckning genom olika internationella överenskommelser, såväl multilaterala som bilaterala. En självklar utgångspunkt är att Sverige på bästa sätt ska fullgöra sina internationella åtaganden i fråga om polisiärt samarbete över gränserna. Med internationella åtaganden avses här folkrättsligt bindande förpliktelser. Sådana åtaganden avser framför allt samarbete med utländska brottsbekämpande myndigheter och med mellanfolkliga organisationer. Samarbetet behöver inte avse brott eller brottslig verksamhet inom den svenska polisens ansvarsområde.

Om det finns ett förpliktande åtagande för polisen att samla in, bearbeta eller lämna ut uppgifter till en utländsk myndighet eller en mellanfolklig organisation måste detta åtagande kunna fullgöras med hjälp av modern teknik. Den nya lagen bör därför ge möjlighet till personuppgiftsbehandling i internationellt samarbete. Mot bakgrund härav föreslås en särskild ändamålsbestämmelse som ger stöd för sådan behandling av personuppgifter.

En stor del av det polisiära samarbetet över gränserna äger rum som ett led i förebyggande, utredning eller lagföring av svensk brottslighet, t.ex. när en svensk myndighet begär rättslig hjälp i en annan stat. Behandlingen av personuppgifter och utlämnandet av information sker då med stöd av de primära ändamålen att förebygga, förhindra eller upptäcka brottslig verksamhet eller att utreda eller beivra brott i Sverige.

Polisens internationella samarbete regleras i en rad olika författningar. Några av de viktigaste är lagen (2000:343) om internationellt polisiärt samarbete, lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar och lagen (2000:344) om Schengens informationssystem. Dessa lagar tar direkt sikte på polisiärt samarbete över gränserna. För att fullgöra åtaganden om sådant samarbete måste polisen kunna behandla personuppgifter i den utsträckning som den konkreta arbetsuppgiften kräver det. Det som regleras i nyssnämnda författningar är främst vilka typer av samarbete som ska förekomma. Hur kommunikationen ska ske ägnas mindre utrymme.

Lagar som reglerar rättslig hjälp, bl.a. lagen (2000:562) om internationell rättslig hjälp i brottmål, lagen (1957:668) om utlämning för brott,

lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge och lagen (2005:500) om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut, bygger också på folkrättsligt bindande överenskommelser. Indirekt ställs det samma krav på behandling av personuppgifter vid rättslig hjälp som vid polisiärt samarbete över gränserna. Enligt den svenska regleringen är det åklagare som ger rättslig hjälp, men i det praktiska utredningsarbetet och vid verkställighet av tvångsmedel anlitar åklagaren biträde av polisen på samma sätt som i en svensk brottsutredning. Det innebär att polisen måste kunna behandla personuppgifter i ett ärende om rättslig hjälp i samma utsträckning som i en förundersökning.

Det internationella samarbetet äger i allt större utsträckning rum genom direktkontakter mellan myndigheterna. En stor del av det polisiära samarbetet sker dock via den internationella kriminalpolisorganisationen ICPO-Interpol (Interpol) eller det polisiära samarbetsorganet inom EU, Europol. Det finns inte några särskilda författningar som reglerar polisens samarbete med dessa organ. De författningsbestämmelser som reglerar samarbetet, och som är av intresse i detta sammanhang, rör informationsutbyte och finns i polisdatalagen, lagen om belastningsregister, lagen om misstankeregister samt lagen om Schengens informationssystem.

Det kan anmärkas att det utbyts stora mängder information i det internationella samarbetet. Som exempel kan nämnas att under år 2007 tog Interpol Stockholm emot 43 500 elektroniska meddelanden och skickade omkring 6 300 meddelanden. Till Sirene-kontoret (Schengen/SIS) inkom ungefär 44 000 meddelanden och skickades omkring 5 000 formulär. Det är således fråga om material i sådan omfattning att det omöjligen kan hanteras manuellt. Åtagandena att lämna och ta emot information måste således kunna fullgöras med hjälp av modern teknik.

Det sagda innebär att det krävs att den nya lagen medger behandling av personuppgifter för att fullgöra internationella åtaganden. Den behandling som åsyftas kan bestå i insamlande och sammanställning av skriftligt material, kontroll i register eller annat. I vissa fall kan det vara fråga om personuppgiftsbehandling som sträcker sig över en längre tid.

På sikt kommer sannolikt en del av dagens informationsutbyte – inom främst EU – att ersättas av system där polismyndigheter i olika länder får direktåtkomst till vissa uppgifter i varandras register. En sådan förändring inverkar dock inte på polisens behov av att kunna behandla uppgifter som ett led i internationellt samarbete.

Rikspolisstyrelsen väcker frågan om Interpol-samarbetet utgör ett sådant internationellt åtagande som avses i promemorians förslag. Interpol är en organisation för polissamarbete som av Förenta Nationerna har erkänts som en mellanstatlig organisation. De förpliktelser för svenskt vidkommande som kan följa med medlemskapet i Interpol får anses vara ett sådant åtagande som, enligt den föreslagna lagen, medger behandling av personuppgifter.

Rikspolisstyrelsen anser också att det bör klargöras att övervakning av vägtrafiken inom ramen för EU-samarbetet omfattas av den föreslagna lagen. Som redovisas i avsnitt 6.3 bör lagens tillämpningsområde omfatta endast den brottsbekämpande verksamheten medan personuppgiftsbehandling i annan polisiär verksamhet ska regleras av personuppgifts-

lagen. Då flera olika verksamheter inom polisen, däribland trafikövervakning, kan utgöra såväl brottsbekämpande som icke-brottsbekämpande verksamhet innebär en sådan gränsdragning att polisen i varje enskilt fall måste ta ställning till syftet med en viss åtgärd eller behandling. I den mån EU-samarbetet ålägger polisen att t.ex. lagra och utbyta trafikövervakningsinformation innehållande personuppgifter får polisen avgöra om behandlingen sker inom ramen för brottsbekämpande verksamhet eller inte. Är det fråga om brottsbekämpande verksamhet omfattas behandlingen av den nya lagen.

7.5 Behandling av uppgifter för diarieföring m.m.

Regeringens förslag: Personuppgifter ska alltid få behandlas om behandlingen är nödvändig för diarieföring eller om uppgifterna har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Utredningens förslag överensstämmer delvis med promemorians. Utredningen föreslår en särskild bestämmelse enligt vilken det alltid ska vara tillåtet att diarieföra personuppgifter och behandla dem i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Med löpande text avses enligt utredningen text som inte har strukturerats så att sökning av personuppgifter underlättas.

Remissinstanserna har inte haft någon invändning mot förslaget.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inte något att invända mot förslaget. *Kustbevakningen* anför att bestämmelsen möjligen bör formuleras på ett annat sätt eftersom begreppet ”diarieföring” inte återfinns i sekretesslagens (numera offentlighets- och sekretesslagen; 2009:400) bestämmelser om registrering och utlämnande av allmänna handlingar. *Sveriges advokatsamfund* efterfrågar förtydliganden och anser bl.a., liksom *Skatteverket*, att det bör klargöras hur förslaget förhåller sig till de föreslagna bestämmelserna om gemensamt tillgängliga uppgifter.

Skälen för regeringens förslag

Det bör införas en särskild ändamålsbestämmelse för diarieföring m.m.

Rikspolisstyrelsen och polismyndigheterna tar dagligen emot stora mängder information av vitt skilda slag, ofta i elektronisk form. De inkommande uppgifterna kan utgöra en del av en allmän handling i tryckfrihetsförordningens mening. Enligt 5 kap. 1 § offentlighets- och sekretesslagen gäller som huvudregel att allmänna handlingar som kommit in till eller upprättats hos en myndighet ska registreras, dvs. diarieföras, så snart som möjligt. Syftet med bestämmelsen är bl.a. att garantera allmänhetens rätt att få tillgång till allmänna handlingar. I 5 kap. 2 § offentlighets- och sekretesslagen uppställs vissa minimikrav beträffande uppgifterna i ett register. När en handling registreras ska det av registret

framgå (1) datum då handlingen kom in eller upprättades, (2) diarienummer eller annan beteckning handlingen fått vid registreringen, (3) i förekommande fall uppgifter om handlingens avsändare eller mottagare och (4) i korthet vad handlingen rör. Utgångspunkten är att dessa uppgifter ska vara tillgängliga för allmänheten. Uppgifterna under punkterna 3 och 4 ska utelämnas eller särskiljas, om det behövs för att registret i övriga delar ska kunna företes för allmänheten.

Vid sidan av skyldigheten att registrera allmänna handlingar gäller enligt förvaltningslagen (1986:223) att en myndighet ska se till att det är möjligt för enskilda att kontakta myndigheten med hjälp av bl.a. e-post och att svar kan lämnas på samma sätt.

Som framgår av avsnitt 7.1 föreslås att ändamålsregleringen utformas så att de primära ändamålen, dvs. de ändamål som ska tillgodose behovet av personuppgiftsbehandling i polisens egen verksamhet, anges uttömmande. Bestämmelserna ger polisen möjlighet att behandla personuppgifter som *behövs* bl.a. för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller beivra brott. När en personuppgift kommer in till en myndighet, t.ex. i ett e-postmeddelande, kan det många gånger vara svårt att avgöra för vilket ändamål, om något, som det finns behov av att behandla uppgiften. I den mån personuppgiften utgör en del av en allmän handling måste den ändå utan dröjsmål kunna behandlas för diarieföring. Därutöver måste myndigheten alltid kunna leva upp till de krav på kommunikation med enskilda som ställs i förvaltningslagen. Det måste alltså finnas en möjlighet att ta emot och diarieföra personuppgifter i elektronisk form, liksom att behandla dem i det ärende som handlingen föranleder, oavsett om myndigheten anser att dessa behövs eller inte.

Mot denna bakgrund bör, som både Polisdatautredningen och promemorian föreslår, det införas bestämmelser som säkerställer att polisen alltid kan diarieföra allmänna handlingar samt ta emot och behandla personuppgifter i en handling i enlighet med förvaltningslagens bestämmelser. Bestämmelserna bör endast ge utrymme för sådan behandling som krävs för en korrekt hantering av en inkommen handling, i huvudsak diarieföring eller mottagande och besvarande av en framställan. Det är således inte möjligt att med stöd av de aktuella bestämmelserna behandla uppgifter i en brottsutredning eller i underrättelseverksamhet. Sådan behandling ska i stället ske med stöd av någon av de övriga ändamålsbestämmelserna. Bestämmelserna om diarieföring m.m. bör utformas i överensstämmelse med promemorians förslag. Uttrycket ”löpande text” bör inte användas i författningstexten, eftersom informationstekniken medger att även texter som inte på förhand har strukturerats på ett visst bestämt sätt kan bli föremål för detaljerade och preciserade sökningar. Av bestämmelserna bör framgå att personuppgifter alltid får behandlas, dels om behandlingen är nödvändig för diarieföring, dels om uppgifterna har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Kustbevakningen pekar på att man i de aktuella bestämmelserna i sekretesslagen inte använder begreppet ”diarieföring” och väcker frågan om bestämmelserna om diarieföring m.m. möjligen bör formuleras om. Det finns enligt regeringens mening inte skäl att frångå promemorians formulering, som tydligt beskriver den behandling som avses. Begreppet

”diarieföring” får vidare anses vara ett vedertaget begrepp för den typ av registrering som regleras i 5 kap. offentlighets- och sekretesslagen.

Förhållandet till bestämmelserna om gemensamt tillgängliga uppgifter

Som diskuteras närmare i avsnitt 9 kommer den föreslagna lagen att skilja mellan personuppgifter som endast ett fåtal personer har tillgång till och personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. För gemensamt tillgängliga uppgifter föreslås lagen innehålla särskilda, mera begränsande, bestämmelser. *Skatteverket* och *Sveriges advokatsamfund* efterfrågar en analys av hur de föreslagna bestämmelserna om diarieföring m.m. förhåller sig till bestämmelserna om gemensamt tillgängliga uppgifter.

Personuppgifter som behandlas med stöd av de föreslagna bestämmelserna om diarieföring m.m. kommer i vissa fall att bli tillgängliga för en större krets personer, t.ex. i diarier. De skulle därmed i och för sig kunna sägas utgöra gemensamt tillgängliga uppgifter. De föreslagna bestämmelserna för gemensamt tillgängliga uppgifter har till syfte att reglera sådan behandling som sker i för verksamheten gemensamma uppgiftssamlingar. Syftet med de nu aktuella ändamålsbestämmelserna är emellertid inte att möjliggöra behandling av personuppgifter i den brottsbekämpande verksamheten i sig. Det är i stället fråga om en särreglering som tar sikte på sådan behandling av personuppgifter som inte ryms i de primära ändamålen men som polisen ändå måste kunna utföra dels för att hantera inkommande handlingar, dels för att tillgodose tryckfrihetsförordningens krav på att allmänheten ska ha tillgång till allmänna handlingar. Flera av de bestämmelser som föreslås gälla vid behandling av gemensamt tillgängliga uppgifter, som t.ex. särskilda upplysningar och sökbegränsningar, är inte lämpade att reglera behandling av personuppgifter i diarier m.m.

Som *Skatteverket* påpekar kan diarieföring inte bara tjäna allmänhetens rätt att få tillgång till allmänna handlingar, utan även tillgodose verksamhetskrav. Den behandling som avses i den föreslagna bestämmelsen om diarieföring omfattar emellertid endast sådan behandling som är nödvändig för diarieföringen. Om det när diarieföringen är avslutad, dvs. när erforderliga uppgifter är registrerade, konstateras att uppgifterna rör polisens brottsbekämpande verksamhet ska den fortsatta behandlingen ske för ett annat i lagen angivet ändamål och i övrigt i överensstämmelse med de allmänna bestämmelserna bl.a. om gemensamt tillgängliga uppgifter. Om således uppgifter i en inkommen handling behövs för viss brottsbekämpande verksamhet, t.ex. i en förundersökning, så får fortsatt behandling ske med stöd av bestämmelserna om personuppgiftsbehandling för det ändamålet. I vilken utsträckning personuppgifterna får göras gemensamt tillgängliga framgår av lagens bestämmelser om gemensamt tillgängliga uppgifter.

I de fall där uppgifter behandlas med stöd av nu aktuell bestämmelse bör de föreslagna reglerna om gemensamt tillgängliga uppgifter inte vara tillämpliga.

7.6 Behandling av uppgifter för att tillhandahålla information till andra

Regeringens förslag: Uppgifter som behandlas i polisens brottsbekämpande verksamhet ska också få behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation,
3. sådan verksamhet hos polisen som avser handräckningsuppdrag,
4. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen,
5. verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten, eller
6. en myndighets verksamhet

a) om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift, eller

b) om tillhandahållandet görs i syfte att samverka mot brott.

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

Utredningen föreslår inte några särskilda bestämmelser om behandling av uppgifter för att tillhandahålla information till andra.

Remissinstanserna: Flera remissinstanser, bl.a. *Tullverket*, har påtalat att polisen och övriga brottsbekämpande myndigheter i allt större omfattning samarbetar inom ramen för brottsbekämpningen och att dessa myndigheter i sin egen brottsbekämpande verksamhet har behov av att få del av uppgifter som finns hos polisen.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorians sekundära ändamål anges dock uttömmande. I promemorian föreslås inte några särskilda ändamål för behandling av uppgifter för att tillhandahålla information till Kriminalvården eller till annan myndighet i syfte att samverka mot brott. Promemorian innehåller inte heller något särskilt ändamål för tillhandahållande av uppgifter till polisens handräckningsverksamhet.

Remissinstanserna: Majoriteten av remissinstanserna har inget att invända mot promemorians förslag. Flera remissinstanser anser dock att de sekundära ändamålen inte i tillräcklig utsträckning tillgodoser polisens behov av att kunna lämna ut uppgifter. *Åklagarmyndigheten* anser att det måste finnas en möjlighet att lämna uppgifter till myndigheter i annat syfte än att bekämpa brott. Som exempel nämns Kriminalvårdens behov av uppgifter av betydelse för säkerheten på kriminalvårdsanstalter. Åklagarmyndigheten föreslår att allt utlämnande som sker med stöd av 14 kap. 3 § sekretesslagen (numera 10 kap. 27 § offentlighets- och sekretesslagen) bör tillåtas.

Även *Rikspolisstyrelsen* konstaterar att det förekommer situationer där andra myndigheter än de som anges i förslaget kan ha behov av uppgifter

från polisens brottsbekämpande verksamhet för sin egen verksamhet. Rikspolisstyrelsen pekar särskilt på sådant utlämnande som sker inom ramen för myndighetsövergripande samverkan mot grov organiserad brottslighet, t.ex. i regionala underrättelsecentrum. Enligt styrelsen bör polisen även fortsättningsvis ha möjlighet att lämna ut uppgifter efter en intresseavvägning enligt 14 kap. 3 § sekretesslagen (numera 10 kap. 27 § offentlighets- och sekretesslagen), exempelvis till Kronofogdemyndigheten, Skatteverket (såväl dess brottsutredande som fiskala del) och Försäkringskassan. Rikspolisstyrelsen lyfter vidare fram behovet av att kunna lämna uppgifter till dels Kriminalvården, t.ex. om uppgiften behövs för att Kriminalvården ska kunna vidta särskilda säkerhetsåtgärder beträffande en intagen, dels Migrationsverket för att verket ska kunna vidta åtgärder i sin verksamhet på utlänningsområdet. Styrelsen nämner bl.a. ett planerat samarbete mellan polisen och migrationsmyndigheter i en Folkrätts- och krigsbrottskommission.

Kriminalvården påpekar att myndigheten har i uppdrag att bekämpa brott under verkställigheten och att upprätthålla säkerheten på anstalter. För att genomföra uppdraget behöver myndigheten kunna få del av uppgifter från polisens brottsbekämpande verksamhet. Kriminalvården anser att det finns starka skäl att överväga om inte Kriminalvården bör räknas till myndigheter med brottsbekämpande verksamhet. *Skatteverket* anser att ändamålen för behandlingen av personuppgifter bör kompletteras. Verket anger bl.a. att det är svårt att överblicka om personuppgiftslagen och den i promemorian föreslagna lagen fullt ut möter de behov av informationsutbyte som har konstaterats i arbetet inom Rådet för rättsväsendets informationsförsörjning, särskilt vad gäller behoven av att planera och följa upp den brottsbekämpande verksamheten. Skatteverket framhåller vidare att en förutsättning för att kunna bekämpa den grova organiserade brottsligheten är bättre möjligheter att utbyta information mellan brottsbekämpande myndigheter och andra myndigheter eller delar av myndigheter. Enligt Skatteverket visar erfarenheter från samverkan i regionala underrättelsecentrum bl.a. på behovet av samverkan mellan Skatteverkets fiskala verksamhet och polisen och skattebrottsenheterna i skedet innan förundersökning. Även *Kronofogdemyndigheten* hänvisar till erfarenheter från samarbete i regionala underrättelsecentrum och anger att det finns skäl att överväga utökade möjligheter till informationsutbyte också med myndigheter som inte är direkt brottsbekämpande.

I fråga om tillhandahållande av information till annan polisiär verksamhet än den brottsbekämpande, delar *Rikspolisstyrelsen* bedömningen att särskilda skäl som huvudregel bör krävas för att personuppgifter ska få tillhandahållas. För att kunna utföra handräckningsuppdrag på ett säkert sätt behöver dock polisen, enligt styrelsen, mer regelmässigt information från den brottsbekämpande verksamheten. *Kriminalvården* framhåller att myndigheten ibland bistår polisen med transporter efter särskilt handräckningsbeslut och betonar att Kriminalvården då behöver de uppgifter om den som ska transporteras som kan ha betydelse för transportens genomförande. *Riksdagens ombudsmän* ifrågasätter om det inte beträffande vissa typer av ärenden hos polisen kan finnas behov av att mera rutinmässigt behandla personuppgifter från den brottsbekämpande verksamheten. I så fall är det angeläget att lagstiftningen ger det

utrymme som behövs, inte minst för att undvika att en restriktiv reglering ”urholkas” i den praktiska tillämpningen.

Några remissinstanser, däribland *Åklagarmyndigheten, Rikspolisstyrelsen* och *Skatteverket*, väcker frågan om det inte bör införas ett särskilt ändamål för behandling av personuppgifter om det behövs för tillsyn, planering och uppföljning.

Skälen för regeringens förslag

Allmänna utgångspunkter

Tidigare har det redovisats hur lagens ändamålsreglering bör utformas och vilka lagens primära ändamål bör vara. I detta avsnitt diskuteras vilka sekundära ändamål som bör anges i lagen. I och med att regleringen av sekundära ändamål inte föreslås vara uttömmande finns ett visst utrymme att lämna ut uppgifter även för andra ändamål än de i lagen angivna, under förutsättning att utlämnandet inte kan anses oförenligt med insamlingsändamålet (finalitetsprincipen). Som tidigare betonats är dock målsättningen att de sekundära ändamålen ska vara så fullständiga som möjligt och omfatta merparten av polisens uppgiftsutlämnande.

I sammanhanget är det viktigt att komma ihåg – vilket *Rikspolisstyrelsen* framhåller – att utlämnande av uppgifter även kan ske inom ramen för något av lagens primära ändamål. Utlämnande av uppgifter till andra kan i många fall vara ett led i den egna verksamheten och således omfattas av de primära ändamålen.

Några remissinstanser, däribland *Rikspolisstyrelsen*, väcker frågan om det behövs en särskild ändamålsbestämmelse som ger stöd för behandling av personuppgifter för bl.a. planering och uppföljning av verksamheten. I lagstiftningsärendet angående lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet uttalade Lagrådet att en sådan bestämmelse är obehövlig (prop. 2004/05:164 s. 179). Lagrådet ansåg att planering, uppföljning och utvärdering av verksamhet är en integrerad del av själva verksamheten och inte någon fristående aktivitet som behöver regleras särskilt. Därför föreslås inte någon sådan ändamålsbestämmelse för polisens vidkommande.

Skatteverket tar upp arbetet inom Rådet för rättsväsendets informationsförsörjning. Med hänsyn till att det är ett pågående arbete är det inte möjligt att nu anpassa den nya lagen till det informationsutbyte som kan komma att föreslås inom ramen för det arbetet.

Tillhandahållande av information till andra brottsbekämpande myndigheter

Det är från brottsbekämpningssynpunkt angeläget att samhällets samlade resurser används på ett så rationellt och effektivt sätt som möjligt. Brottsligheten känner inga geografiska gränser eller myndighetsgränser. Att brottsbekämpande myndigheter bör samverka framstår därför som självklart. Lika självklart är att en sådan samverkan förutsätter möjligheter till effektivt utbyte av information.

Regeringen har tagit initiativ till en nationell mobilisering mot den grova organiserade brottsligheten. I en departementspromemoria med samma namn ges förslag på åtgärder för en effektivare och mer uthållig bekämpning av denna typ av brottslighet (Ds 2008:38). En av de viktigaste åtgärderna som lyfts fram är just ökad samverkan mellan myndigheter. Samtliga brottsbekämpande myndigheter framhåller också i sina remissvar i detta lagstiftningsärende betydelsen av en utvecklad samverkan.

Ett väl fungerande informationsutbyte skapar förutsättningar att se kopplingar mellan brottslighet inom skilda myndigheters ansvarsområden. Det är därför viktigt att den moderna teknikens möjligheter kan tas till vara för sådant informationsutbyte. Möjligheterna att få tillgång till underrättelseinformation genom direktåtkomst bör förbättras. De risker för intrång i den personliga integriteten som direktåtkomst och andra former av elektroniskt informationsutbyte kan ge upphov till och hur dessa risker bör hanteras diskuteras i avsnitt 12.

Mot denna bakgrund bör det i den nya lagen uttryckligen anges att de uppgifter som förekommer i polisens brottsbekämpande verksamhet får behandlas för att tillhandahålla information som andra brottsbekämpande myndigheter behöver i sin brottsbekämpande verksamhet. Motsvarande bestämmelser finns i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och i den förordning som reglerar behandling av personuppgifter i Åklagarmyndighetens verksamhet. I avsnitt 13 föreslås sekretessbrytande bestämmelser som ska gälla i förhållande till andra brottsbekämpande myndigheter.

Tillhandahållande av information till annan myndighet i syfte att samverka mot brott

En effektiv brottsbekämpning förutsätter samverkan inte bara mellan myndigheter som har till uppgift att bekämpa brott utan även mellan brottsbekämpande myndigheter och andra myndigheter. Som flera remissinstanser framhåller, däribland *Rikspolisstyrelsen, Skatteverket* och *Kronofogdemyndigheten*, sker sådan samverkan t.ex. i regionala underrättelsecentrum (jfr avsnitt 7.2 om sådan samverkan). Vilka myndigheter som är representerade i underrättelsecentrum varierar. Kronofogdemyndigheten, Skatteverkets fiskala del, Kriminalvården, Migrationsverket och Försäkringskassan är exempel på myndigheter som deltar i sådan samverkan.

I departementspromemorian om nationell mobilisering mot den grova organiserade brottsligheten betonas behovet av ökad samverkan mellan myndigheter. Arbetet har övergått i en genomförandefas, sedan regeringen gett Rikspolisstyrelsen i uppdrag att vidta åtgärder för att säkerställa en effektiv och uthållig verksamhet för bekämpning av den grova organiserade brottsligheten (dnr Ju2008/5776/PO). Av slutredovisningen av uppdraget framgår bl.a. att det har etablerats permanenta regionala underrättelsecentrum på åtta platser i landet samt att ett samverkansråd och ett operativt råd har inrättats med bred myndighetsrepresentation (dnr Ju2009/5516/PO).

Myndighetssamverkan förutsätter utbyte av information. Ofta är det tillräckligt med avidentifierade uppgifter men i den operativa verksamheten kan det vara nödvändigt att utbyta information som innehåller personuppgifter. Det ter sig mer betänkligt från integritetsskyddssynpunkt att tillåta polisen att tillhandahålla personuppgifter från den brottsbekämpande verksamheten till andra myndigheter än de som har till uppgift att bekämpa brott. Som flera remissinstanser påpekar förekommer dock redan nu ett sådant uppgiftsutlämnande efter en intresseavvägning enligt 10 kap. 27 § offentlighets- och sekretesslagen.

Polisen bör även fortsättningsvis ges möjlighet att behandla uppgifter för att tillhandahålla information till andra än brottsbekämpande myndigheter, när syftet är att samverka mot brott. Information bör få tillhandahållas om utlämnandet kan vara till nytta för den brottsbekämpande verksamheten. Begreppet samverkan kan omfatta flera olika former av samarbete. Samverkan kan avse såväl diskussioner i strategiska frågor som mer operativt samarbete, t.ex. en planerad gemensam aktion. Ett exempel på samverkan är arbetet i underrättelsecentrum. Ett annat exempel är samverkan mellan polisen, Tullverket, Kustbevakningen och Migrationsverket vid gränskontroll.

Av skäl som anges i avsnitt 13 bör det inte införas några sekretessbrytande bestämmelser i förhållande till andra myndigheter än de brottsbekämpande.

Tillhandahållande av information till utländska brottsbekämpande myndigheter eller organisationer

Inom ramen för det internationella polissamarbetet måste polisen kunna behandla personuppgifter för att lämna ut dem i den utsträckning det behövs för att fullgöra internationella åtaganden eller om det annars är förenligt med svenska intressen. Det kan exempelvis vara fråga om att på begäran översända uppgifter till Interpol eller att lämna upplysningar till en utländsk myndighet om vilka åtgärder som har vidtagits i Sverige med anledning av utländsk information. Eftersom det internationella informationsutbytet förutsätter att uppgifter i vissa fall kan lämnas utan föregående förfrågan från en annan stat, bör det vara möjligt att behandla och lämna ut uppgifter även om detta endast är ett allmänt åtagande enligt en överenskommelse men inte ett bindande krav. Sådan behandling bör även, liksom för närvarande, vara möjlig när det inte finns någon överenskommelse som reglerar uppgiftsutlämnandet, t.ex. för att kunna varna en polismyndighet i ett annat land om ett förestående brott i det landet. I lagen bör det därför tas in en bestämmelse om att uppgifter får behandlas, om det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation. I avsnitt 12 och 13 diskuteras olika frågor som rör informationsutbyte och sekretess i det internationella samarbetet.

Tillhandahållande av information till Kriminalvården

Kriminalvården har bl.a. till uppgift att verka för att påföljder verkställs på ett säkert sätt och att återfall i brott förebyggs. Myndigheten är enligt

2 § förordningen (2007:1172) med instruktion för Kriminalvården skyldig att vidta särskilda åtgärder för att förhindra brottslighet under verkställigheten. Enligt 3 § 3 lagen (2001:617) om behandling av personuppgifter inom Kriminalvården får personuppgifter behandlas om det behövs för att upprätthålla säkerheten och förebygga brott bl.a. under den tid som en person är häktad eller intagen i kriminalvårdsanstalt. För detta ändamål ska Kriminalvården enligt 39 § förordningen (2001:682) om behandling av personuppgifter inom Kriminalvården föra ett särskilt register benämnt säkerhetsregistret.

I förarbetena till Kriminalvårdens registerlagstiftning anfördes att framväxten av kriminella sammanslutningar och nätverk förutsätter samarbete mellan Kriminalvården och polisen (prop. 2000/01:126 s. 27). Att det behövs uppgiftsutbyte mellan polisen och Kriminalvården lyfts även fram av Rymningsutredningen (SOU 2005:6 s. 120) och av Beredningen för rättsväsendets utveckling (SOU 2005:117 s. 202 f.). Det finns således ett behov av uppgiftsutbyte mellan polisen och Kriminalvården. Det är t.ex. viktigt att Kriminalvården kan få upplysningar från polisen för att kunna göra riktiga bedömningar bl.a. när det gäller placering av intagna och beslut om permissioner.

Polisen bör därför ges möjlighet att behandla uppgifter om det är nödvändigt för att tillhandahålla Kriminalvården sådan information som myndigheten behöver i sin verksamhet för att förebygga brott och upprätthålla säkerheten, bl.a. på häkten och kriminalvårdsanstalter. Flera remissinstanser, däribland *Rikspolisstyrelsen* och *Kriminalvården,* framhåller också vikten av att den nya lagen tillåter sådan behandling.

Tillhandahållande av information till annan polisiär verksamhet

För att polisen ska kunna fullgöra arbetsuppgifter som faller utanför den brottsbekämpande verksamheten behöver man ibland ha tillgång till uppgifter som har samlats in för brottsbekämpande ändamål. Uppgifter som behandlas inom den brottsbekämpande verksamheten behöver alltså i viss utsträckning kunna tillhandahållas till annan polisverksamhet.

Polisen har i varierande utsträckning tillgång till uppgifter i misstankeregistret och belastningsregistret i olika typer av förvaltningsärenden. Tillgången till uppgifter är anpassad för att svara mot de normala behoven av information. I vissa fall finns det emellertid annan information hos polisen som kan vara viktig, exempelvis underrättelseinformation. En person kan t.ex. ha sådana kontakter i kriminella kretsar att denne vid en helhetsbedömning ter sig olämplig som befattningshavare, tillståndshavare eller liknande. Det framstår därför som rimligt att polisen i viss utsträckning ska kunna lämna över uppgifter från den brottsbekämpande verksamheten till annan polisiär verksamhet. Om någon som ska besluta i ett förvaltningsärende begär information från den brottsbekämpande verksamheten har denne med stöd av 6 kap. 5 § offentlighets- och sekretesslagen rätt att få ut uppgifterna, om inte sekretess hindrar det (se nedan). Det förutsätter dock att beslutsfattaren har vetskap om att det finns någon information som kan ha betydelse. Frågan är i vilken utsträckning uppgifter även ska få tillhandahållas utan föregående begäran.

De områden där polisen, typiskt sett, kan ha behov av att få del av information som har samlats in i den brottsbekämpande verksamheten gäller bl.a. arbete med att (1) förordna vissa befattningshavare, t.ex. arrestantvakter, (2) pröva tillståndsärenden, (3) fullgöra sin skyldighet enligt författning att bistå andra myndigheter (handräckningsskyldighet), och (4) besluta om att en tvångsåtgärd enligt t.ex. djurskyddslagen (1988:534) eller utlänningslagen (2005:716) ska verkställas vid fara i dröjsmål.

Som anförs i promemorian bör det som huvudregel krävas särskilda skäl för att tillhandahålla personuppgifter från den brottsbekämpande verksamheten till annan polisiär verksamhet, vilket också *Rikspolisstyrelsen* ställer sig bakom. Därigenom tydliggörs att överlämnandet kräver särskild eftertanke. Kravet på särskilda skäl bör dock, som *Riksdagens ombudsmän* påpekar, inte gälla för tillhandahållande av personuppgifter till verksamhet som mera rutinmässigt behöver uppgifter från den brottsbekämpande verksamheten. Enligt Rikspolisstyrelsen är så fallet för den verksamhet som består i att utföra handräckningsuppdrag åt andra myndigheter. Styrelsen framhåller att polisen behöver omfattande information, däribland information från den brottsbekämpande verksamheten, för att förebygga och minska risken att personer kommer till skada m.m. vid genomförandet av sådana uppdrag. Informationen behövs för att handräckningsåtgärden ska kunna planeras och anpassas efter den person som åtgärden avser och omständigheterna i övrigt. Även *Kriminalvården*, som ibland bistår polisen med vissa transporter efter särskilda handräckningsbeslut, framhåller behovet av information från den brottsbekämpande verksamheten för detta ändamål.

Eftersom det finns behov av att mera rutinmässigt tillhandahålla information till polisens handräckningsverksamhet bör det inte ställas upp något krav på särskilda skäl för att tillhandahålla personuppgifter till sådan verksamhet. Här kan också erinras om att uppgifter som polisen mottar i viss sådan verksamhet omfattas av sekretess enligt 35 kap. 20 § första stycket 2, 3, 4 och 5 offentlighets- och sekretesslagen.

Tillhandahållande av information till myndigheter i vissa andra fall

Det finns även vissa andra fall där personuppgifter bör få behandlas av polisen för utlämnande till andra. Enligt 10 kap. 15 § offentlighets- och sekretesslagen hindrar sekretess inte att uppgift lämnas till regeringen eller riksdagen. Det bör därför i den nya lagen anges att personuppgifter får behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen. Det bör även anges att uppgifter får behandlas för att lämnas ut till andra, om det enligt lag eller förordning åligger polisen att tillhandahålla sådan information. Med andra avses såväl myndigheter som enskilda. Med skyldighet att lämna ut uppgifter avses dels uppgiftsskyldighet enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen, dels andra författningsreglerade skyldigheter att lämna ut uppgifter. Enligt 6 kap. 5 § offentlighets- och sekretesslagen ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. Enligt promemorian

innefattar denna bestämmelse (dåvarande 15 kap. 5 § sekretesslagen) inte en uppgiftsskyldighet i nu aktuellt hänseende. I flera lagstiftningsärenden därefter har dock en motsatt bedömning gjorts (se t.ex. prop. 2008/09:96 s. 80). Mot den bakgrunden får 6 kap. 5 § offentlighets- och sekretesslagen anses innefatta en sådan skyldighet att lämna uppgifter som avses i den nya lagen.

Åklagarmyndigheten anser att det alltid bör vara tillåtet att behandla uppgifter för att kunna lämna ut dem med stöd av 14 kap. 3 § sekretesslagen (numera 10 kap. 27 § offentlighets- och sekretesslagen). Det kan konstateras att polisens uppgiftslämnande enligt 10 kap. 27 § offentlighets- och sekretesslagen i flertalet fall omfattas av de mer preciserade sekundära ändamål som anges i lagen. I den mån det är fråga om uppgiftslämnande på begäran av annan myndighet kan uppgiftslämnande enligt den paragrafen dessutom, som nyss nämnts, ske med stöd av 6 kap. 5 § offentlighets- och sekretesslagen. Därutöver kan uppgiftslämnande ske om det är förenligt med finalitetsprincipen.

Polisen måste även ha möjlighet att behandla personuppgifter, om det behövs för att fullgöra författningsenliga förpliktelser att bistå en annan svensk myndighet. Detta kan exempelvis bli aktuellt när polisen bistår Riksdagens ombudsmän och Justitiekanslern med uppgifter i de fall där dessa uppträder som förundersökningsledare och åklagare. En bestämmelse om detta bör tas in i lagen.

Möjlighet för regeringen att meddela föreskrifter

Enligt 17 § polisdataförordningen (1999:81) har polisen möjlighet att till vissa myndigheter lämna ut uppgifter om efterlysta personer och avlägsnanden ur riket. Där föreskrivs även en möjlighet att till konkursförvaltare lämna ut uppgifter i en förundersökning som kan antas ha betydelse för en konkursutredning. Den nya lagen bör innehålla en bestämmelse som erinrar om att regeringen har möjlighet att meddela sådana föreskrifter.

8 Behandling av känsliga personuppgifter

Regeringens förslag: Uppgifter om en person ska inte få behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Uppgifter om en person som behandlas på annan grund ska dock få kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Känsliga personuppgifter ska också få behandlas, om detta är nödvändigt för diarieföring eller om uppgifterna har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

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

Utredningens förslag överensstämmer i huvudsak med promemorians.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt förslaget eller inte haft några invändningar mot det. *Ombudsmannen mot diskriminering på grund av sexuell läggning* har ansett att begreppet sexuell läggning inte bör användas utan ersättas med något annat begrepp, exempelvis sexualliv eller sexuellt beteende.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inget att invända mot förslaget. *Sveriges advokatsamfund* frågar sig i vilken utsträckning behandling av känsliga uppgifter kan ske med stöd av undantaget för behandling som är nödvändig för handläggningen. *Journalistförbundet* framhåller att behandling av känsliga uppgifter måste ske med yttersta försiktighet och föreslår att det införs en skyldighet för regeringen att varje år till riksdagen rapportera de avsteg som gjorts från förbudet att behandla känsliga personuppgifter och ange i vilken utsträckning avstegen har varit effektiva i den brottsbekämpande verksamheten.

Skälen för regeringens förslag: I lagstiftning om behandling av personuppgifter har känsliga personuppgifter en särställning. Enligt 5 § polisdatalagen (1998:622) 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 sexuella läggning. Om uppgifter om en person redan behandlas på annan grund, får dock uppgifterna kompletteras med sådana uppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen. Paragrafen överensstämmer med Europarådets rekommendation No. R (87) 15 om användning av personuppgifter inom polissektorn m.m. (se avsnitt 4.2.3). Innebörden av 5 § polisdatalagen är att det t.ex. inte är tillåtet att föra särskilda register över personer med viss sexuell läggning. Förekommer personen i en förundersökning eller något annat ärende, får dock uppgiften om sexuell läggning antecknas, om det bedöms vara oundgängligen nödvändigt för syftet med behandlingen.

Bestämmelserna i 5 § polisdatalagen bör föras över till den nya lagen. På motsvarande sätt som i personuppgiftslagen och lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet bör dock uttrycket sexualliv användas i stället för sexuell läggning. Vidare bör uttrycket oundgängligen ersättas med absolut. Slutligen bör det i lagtexten framhållas att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt och med respekt för människovärdet.

Riksdagen har uttalat att det inte finns någon vetenskaplig grund för att dela in människor i skilda raser och ur biologisk synpunkt följaktligen heller ingen grund för att använda ordet ras om människor. Användningen av ordet ras i författningstexter riskerar enligt riksdagen att underblåsa fördomar. Riksdagen har dock, med anledning av ett krav i en motion, konstaterat att den inte har möjlighet att besluta att ordet ska utmönstras ur all lagstiftning, eftersom det så gott som uteslutande används i författningar som grundas på internationella överenskommelser eller författningar som genomför EG-direktiv (bet. 1997/98:KU29 s. 7). Användningen av ordet ras har även kritiserats i propositionen till den nya diskrimineringslagen (prop. 2007/08:95 s. 117) och i betänkandet En

reformerad grundlag (SOU 2008:125, Del 1, s. 412). Det saknas underlag att i detta lagstiftningsärende utmönstra ordet ras och därmed ändra den vedertagna beskrivningen av känsliga personuppgifter, jfr t.ex. 13 § personuppgiftslagen (1998:204) och 11 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Som framgår av nyssnämnda proposition är det dock regeringens ambition att i ett annat sammanhang se över frågan om huruvida ordet ras bör utmönstras i all lagstiftning.

Polisen måste alltid ha möjlighet att diarieföra och handlägga inkommande anmälningar och liknande skrivelser. Skälen för detta har utvecklats i avsnitt 7.5. Sådan behandling bör vara tillåten även i de fall där inkommande anmälningar innehåller känsliga personuppgifter. Detta bör komma till uttryck i lagtexten som ett undantag från förbudet att behandla känsliga personuppgifter. I nyss nämnda avsnitt redogörs för vilken behandling som bör omfattas av bestämmelsen om behandling för diarieföring.

Journalistförbundet föreslår att regeringen bör åläggas att årligen rapportera till riksdagen vilka avsteg som gjorts från förbudet att behandla känsliga personuppgifter. Kontrollen av att regleringen följs bör enligt regeringens mening i första hand utövas av tillsynsmyndigheter. I avsnitt 17.2 föreslås en utökad tillsyn över polisens behandling av personuppgifter. Enligt förslaget ska Säkerhets- och integritetsskyddsnämndens tillsyn särskilt avse polisens behandling av känsliga personuppgifter. Skäl för en sådan rapportering som Journalistförbundet efterlyser saknas således.

I avsnitt 11.2 behandlas frågan om användning av känsliga personuppgifter som sökbegrepp.

9 Gemensamt tillgängliga uppgifter

9.1 Särskilda regler för behandling av gemensamt tillgängliga uppgifter

Regeringens förslag: I stället för bestämmelser om register och databaser ska den nya lagen innehålla särskilda regler om behandling av uppgifter som görs eller har gjorts *gemensamt tillgängliga* i den brottsbekämpande verksamheten. Bestämmelserna ska framför allt reglera sådan behandling av uppgifter som sker i för verksamheten gemensamma uppgiftssamlingar. Behandling som utförs av en enskild tjänsteman eller inom en begränsad grupp personer, t.ex. genom vanlig ordbehandling eller genom e-postkommunikation, ska inte omfattas av dessa bestämmelser. Registerbegreppet behålls för vissa särskilda fall.

Bestämmelserna om gemensamt tillgängliga uppgifter ska inte gälla när personuppgifter behandlas med stöd av bestämmelserna om diarieföring m.m.

Utredningens förslag innehåller inte några bestämmelser som särskilt avser gemensamt tillgängliga uppgifter.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian tydliggör dock inte förhållandet mellan bestämmelserna om gemensamt tillgängliga uppgifter och de föreslagna bestämmelserna om behandling av personuppgifter för diarieföring m.m.

Remissinstanserna: Majoriteten av remissinstanserna ställer sig bakom promemorians förslag eller har inget att invända mot det. Flera remissinstanser, däribland *Kustbevakningen* och *Tullverket*, välkomnar att det föreslås ett teknikneutralt begrepp nämligen ”gemensamt tillgängliga uppgifter” i stället för uttryck som register, databas eller uppgiftssamling. *Åklagarmyndigheten* har ingen invändning mot förslagets indelning av uppgifter som är gemensamt tillgängliga och sådana som inte är det och anser att regleringen av vilka uppgifter som får göras gemensamt tillgängliga synes ändamålsenlig.

Några remissinstanser, bl.a. *Riksdagens ombudsmän* och *Uppsala universitet,* anser att det är svårt att dra en gräns mellan uppgifter som är gemensamt tillgängliga och sådana som inte är det. Myndigheterna anser att avgränsningsfrågorna bör avgöras i lagstiftningsärendet. Enligt Riksdagens ombudsmän måste utrymmet att överlämna till Rikspolisstyrelsen att ge interna riktlinjer till förtydligandet av begreppet gemensamt tillgängliga uppgifter vara utomordentligt begränsat med hänsyn till avgränsningens betydelse från integritetsskyddssynpunkt. Även Uppsala universitet ifrågasätter om det är rätt väg att gå att låta användarna styra konstruktionen av ett system som det här aktuella.

Riksdagens ombudsmän anser att det bör vara ensamt avgörande för avgränsningen av gemensamt tillgängliga uppgifter om uppgifterna är åtkomliga för en bestämd och begränsad personkrets eller inte. Enligt Riksdagens ombudsmän kan ett fåtal personer inte betyda så många personer som ett tiotal.

Rikspolisstyrelsen påpekar att de föreslagna bestämmelserna om gemensamt tillgängliga uppgifter kommer att bli tillämpliga på en stor del av behandlingen av uppgifter i den polisiära verksamheten. Sådan behandling som sker i s.k. särskilda undersökningar och andra underrättelseprojekt kommer t.ex. enligt styrelsen i normalfallet att omfattas av bestämmelserna. Mot denna bakgrund anser styrelsen att vissa av bestämmelserna som föreslås gälla för gemensamt tillgängliga uppgifter är för begränsande.

Kustbevakningen och *Skatteverket* invänder mot att bestämmelserna om gemensamt tillgängliga uppgifter gäller så snart en tjänsteman från en annan myndighet än polisen är delaktig i behandlingen av personuppgifter. Myndigheterna anser att ett fåtal tjänstemän från olika myndigheter bör kunna arbeta tillsammans i ett underrättelseprojekt utan att de mer begränsande bestämmelserna, t.ex. om sökbegränsningar, blir tillämpliga.

Datainspektionen anser att även antalet uppgifter och deras struktur bör beaktas vid bedömningen av om uppgifter är att anse som gemensamt tillgängliga. Vidare menar inspektionen att bestämmelserna om gemensamt tillgängliga uppgifter bör tillämpas vid insamlandet av uppgifter, om de insamlade uppgifterna är avsedda att göras gemensamt tillgängliga eller om det kan antas att de kommer att bli det. Bestämmelserna bör alltid tillämpas i polisens kriminalunderrättelseverksamhet. Inspektionen

anser att det angivna antalet om ett tiotal personer som får ha tillgång till uppgifter som inte är gemensamt tillgängliga är alltför stort.

Sveriges advokatsamfund vänder sig mot den komplexa regelstruktur som de snabbt framväxande registerlagarna i allt högre grad kommit att präglas av och pekar bl.a. på bristande enhetlighet i begreppsbildningen. Som exempel nämns att uppgiftssamlingar har betecknats och avgränsats på vitt skilda sätt. Advokatsamfundet efterlyser klargöranden i fråga om skillnaderna mellan den behandling av personuppgifter som avses ske i egentliga register respektive i löpande text samt hur behandling av elektroniska dokument i elektroniska akter avses att regleras.

Skälen för regeringens förslag

Gemensamt tillgängliga uppgifter – ett nytt begrepp

Den nya lagen kommer att gälla för all automatiserad behandling av personuppgifter i polisens brottsbekämpande arbete. Detta innebär att inte bara uppgifter som behandlas i för verksamheten gemensamma uppgiftssamlingar, t.ex. register eller ärendehanteringssystem, ska omfattas utan även sådan behandling som utförs av en enskild tjänsteman eller en begränsad grupp personer, t.ex. vanlig ordbehandling och e-postkommunikation. Risken för otillbörliga intrång i den personliga integriteten är större när personuppgifter används av flera gemensamt i verksamheten än när personuppgifter behandlas av en enskild tjänsteman vid den egna datorn utan att någon annan har åtkomst till uppgifterna. Det är därför nödvändigt att införa särskilda och mer begränsande regler för behandling av uppgifter som används av eller i vart fall är tillgängliga för fler än ett fåtal personer.

Frågan är då hur man bör avgränsa den personuppgiftsbehandling för vilken mera begränsande regler är nödvändiga.

I tidigare lagstiftning om personuppgiftsbehandling har begreppen register och databas använts för att definiera uppgifter som har gjorts tillgängliga för en större krets. Till respektive register har sedan knutits regler om åtkomst, sökmöjligheter m.m. Registerbegreppet har dock kritiserats, bl.a. därför att det har en teknisk anknytning och därför att dagens datasystem normalt inte byggs som traditionella register. Också begreppet databas har en stark teknisk anknytning och leder tanken till ett visst, i tekniskt avseende avgränsat, informationssystem. Detta är inte ett helt relevant sätt att se på samlingar av uppgifter i elektronisk form. Uppgifter kan t.ex. införas helt ostrukturerat och oorganiserat i olika filer i en dator, utan att detta förhindrar en effektiv hantering av uppgifterna för olika sammanställningar m.m. Även om registerbegreppet fortsättningsvis kommer att användas inom polisen för vissa särskilda fall (bl.a. för några av de register som undantas från den nya lagens tillämpningsområde samt register över DNA-profiler) går utvecklingen mot att registerformen överges för mer sofistikerade datasystem.

Som en följd av detta bör den nya regleringen inte bygga på att behandlingen av personuppgifter sker i olika register eller databaser utan i stället ges en mera generell utformning. Ett tänkbart alternativ är att skapa särskilda begränsande regler för personuppgiftsbehandling som avser ”samlingar av uppgifter” eller ”uppgiftssamlingar”. Begreppet upp-

giftssamling används i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Begreppet är dock inte ändamålsenligt för polisens del, bl.a. därför att det kan ge intryck av att det finns i förväg definierade och avgränsade uppgiftssamlingar för all behandling i den brottsbekämpande verksamheten, trots att så inte är fallet. Eftersom den nya regleringen ska omfatta all automatiserad behandling i polisens brottsbekämpande verksamhet, bör ett annat begrepp väljas. I betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18) föreslås i stället för uttryck som databas, register eller uppgiftssamling begreppet *gemensamt tillgängliga uppgifter* för att uttrycka samma sak. Detta begrepp föreslås även av Åklagardatautredningen i förslaget till lag om behandling av uppgifter i åklagarväsendets brottsbekämpande verksamhet (SOU 2008:87).

Det väsentliga i sammanhanget är inte på vilket sätt uppgifter tekniskt lagras utan den faktiskt åsyftade tillgängligheten. Den form av behandling som ska särskiljas bör därför definieras med avsikt på det faktiska förhållande som är avgörande för behovet av särreglering, nämligen att uppgifterna är gemensamt tillgängliga i verksamheten. Den nya lagen bör därför innehålla särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. Med den formuleringen görs det klart att det viktiga inte är var uppgiften rent tekniskt är lagrad eller behandlas, utan om ett flertal personer har möjlighet att ta del av uppgiften. I och med att uttrycket gemensamt tillgänglig uteslutande har en rättslig innebörd understryks lagstiftningens teknikneutralitet. Som framgår i avsnitt 6.1 bör en utgångspunkt vara att den nya lagen inte ska reglera hur uppgifterna tekniskt organiseras, utan endast utgöra en rättslig ram för vilka uppgifter som får behandlas och på vilket sätt de får användas. Polisen bör kunna välja mellan att skapa ett stort centralt datasystem eller flera mindre system eller en blandning av båda alternativen. Det kan t.ex. vara fråga om både ärendehanteringssystem med elektroniska akter och handlingar och traditionella register med eller utan fritextfält. Den nya lagen bör således inte, som *Sveriges advokatsamfund* synes utgå ifrån, reglera vilken behandling som får ske i ”egentliga” register respektive i löpande text. Inte heller bör det i lagen införas några särskilda bestämmelser om elektroniska handlingar eller elektroniska akter.

Det vore, som Sveriges advokatsamfund framhåller, en fördel om samma grundläggande begrepp används i myndigheters registerförfattningar, och kanske särskilt i de som gäller för de brottsbekämpande myndigheterna. Några tillämpningsproblem vad gäller begreppet gemensamt tillgängliga uppgifter torde dock inte uppkomma i förhållande till andra registerlagar, jämför t.ex. lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet där begreppet databas används för att beskriva att uppgifter är tillgängliga för flera. Betänkandena med förslag till lagar om behandling av personuppgifter hos Kustbevakningen respektive åklagarväsendet föreslår också, som nyss nämnts, att begreppet gemensamt tillgängliga uppgifter används.

Gränsdragningen mellan behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga och annan behandling

Det ligger i sakens natur att det inte är enkelt att dra en tydlig gräns mellan uppgifter som är gemensamt tillgängliga och andra uppgifter. Som *Riksdagens ombudsmän* och *Uppsala universitet* understryker bör avgränsningsfrågorna behandlas så ingående som möjligt i lagstiftningsärendet. Riksdagens ombudsmän betonar att det avgörande bör vara om uppgifterna är åtkomliga för en bestämd och begränsad personkrets eller inte. I det följande anges de principer som bör ligga till grund för gränsdragningen.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga bör vara att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Uppgifter som endast ett fåtal personer har rätt att ta del av bör dock inte anses som gemensamt tillgängliga. Att en uppgift ”är tillgänglig” för en viss person bör förstås så att personen har såväl faktisk möjlighet att ta del av uppgiften som rättslig behörighet till det. Det bör däremot inte spela någon roll hur många personer som faktiskt tar del av de aktuella uppgifterna. Det bör inte heller ha någon betydelse om den som har tillgång till uppgiften kan påverka den eller bara läsa den.

Detta innebär till att börja med att personuppgifter blir att anse som gemensamt tillgängliga om dessa behandlas för att en obestämd krets – t.ex. hela polisorganisationen – ska kunna ta del av uppgifterna. De centrala register som Rikspolisstyrelsen för har just syftet att tillgodose informationsbehovet inom olika delar av organisationen. Som exempel på sådana befintliga register kan nämnas det allmänna spaningsregistret, det centrala kriminalunderrättelseregistret och det centrala brottsspaningsregistret. I dessa och liknande system lagras personuppgifter på ett sådant sätt att många anställda har möjlighet att vid behov kunna ta del av uppgifterna, t.ex. under arbetet med en förundersökning eller för att genomföra ett underrättelseprojekt. På liknande sätt kommer uppgifter som är avsedda för en hel polismyndighet eller för en viss enhet inom polisorganisationen normalt att anses som gemensamt tillgängliga. Som exempel kan nämnas lokala system som Rationell anmälningsrutin (RAR) som innehåller brottsanmälningar och Datoriserad utredningsrutin (DurTvå) som innehåller förundersökningar. Detta innebär exempelvis att de flesta förundersökningar redan från början kommer att vara gemensamt tillgängliga, även om det bara är ett fåtal handläggare som arbetar med förundersökningen. Också andra uppgifter som är tillgängliga för en i förväg obestämd krets av personer bör, som huvudregel, anses gemensamt tillgängliga. Begreppet ”gemensamt tillgängliga uppgifter” kommer att täcka inte enbart register i traditionell bemärkelse utan alla uppgiftssamlingar som är avsedda för en obestämd krets av personer.

Vidare bör personuppgifter anses vara gemensamt tillgängliga även i vissa fall när den personkrets som har tillgång till uppgifterna är bestämd och avgränsad. Om uppgifterna är tillgängliga för ett stort antal bestämda personer, bör de således anses vara gemensamt tillgängliga. De personuppgifter som behandlas i brottsbekämpande verksamhet som involverar ett flertal tjänstemän som gemensamt behandlar viss information bör alltså regelmässigt anses som gemensamt tillgängliga. Uppgifter bör

dock inte anses som gemensamt tillgängliga enbart därför att två eller flera personer har tillgång till dem. Kan man redan från början konstatera att personuppgifterna endast kommer att vara tillgängliga för en avgränsad krets bestående av en handfull personer, bör uppgifterna alltså *inte* anses som gemensamt tillgängliga. De integritetsskyddsintressen som motiverar särskilda regler för gemensamt tillgängliga uppgifter gör sig inte lika starkt gällande när bara ett fåtal personer har tillgång till uppgifterna som när många personer har tillgång till dem. En jämförelse kan härvid göras med den relativt omfattande personuppgiftsbehandling som tillåts inom ramen för en särskild undersökning med stöd av 14–16 §§ polisdatalagen (1998:622).

En förutsättning för att uppgifterna inte ska anses vara gemensamt tillgängliga måste dock vara att kretsen som har tillgång till dem omfattar endast ett litet antal personer. Så kan vara fallet t.ex. med ett mindre underrättelseprojekt. Om projektet enbart engagerar en avgränsad krets, bestående av ett fåtal på förhand utpekade personer eller funktioner, bör de uppgifter som behandlas inom ramen för projektet normalt inte betraktas som gemensamt tillgängliga. Så snart det är fråga om mer än ett fåtal personer som har tillgång till uppgifterna bör utgångspunkten vara den motsatta.

Promemorian anger som en tumregel att uppgifter normalt bör anses som gemensamt tillgängliga när fler än ett tiotal personer har tillgång till dem. Promemorian använder i detta sammanhang uttrycket ”ett fåtal bestämda personer”. *Riksdagens ombudsmän* anser att så många som ett tiotal personer inte kan anses utgöra ett fåtal personer och *Datainspektionen* menar att antalet bör begränsas till färre än ett tiotal. Åklagardatautredningen anser, liksom promemorian, att storleken på personkretsen som har tillgång till en uppgift bör vara grundläggande för bedömningen av om en uppgift ska anses vara gemensamt tillgänglig eller inte. Utredningen anser dock att det inte är lämpligt att ange en allomfattande gräns för när personkretsen ska medföra det ena eller andra utfallet av bedömningen och menar att verksamheten vid den enskilda myndigheten bör vara avgörande för gränsen för storleken på personkretsen (SOU 2008:87 s. 181).

Enligt regeringens mening bör, som Åklagardatautredningen anför, det inte i lag anges någon exakt gräns för antalet personer. Även andra omständigheter bör i det enskilda fallet bör kunna vägas in i bedömningen av om personuppgifter ska betraktas som gemensamt tillgängliga eller inte. Som några remissinstanser, bl.a. *Riksdagens ombudsmän,* påpekar är det dock viktigt från integritetsskyddssynpunkt att det i lagstiftningsärendet anges tydliga riktlinjer för gränsdragningen mellan gemensamt tillgängliga uppgifter och andra uppgifter. Det är därför lämpligt att ange en tumregel för hur många personer ett fåtal kan anses utgöra. Promemorians förslag om ett tiotal personer får, i fråga om polisens verksamhet, anses väl avvägt.

När det talas om en bestämd krets bör detta inte uppfattas som att det alltid från början måste kunna anges exakt vilka tjänstemän eller vilken krets av tjänstemän som avses få tillgång till uppgifterna. Bedömningen blir naturligtvis enklare om man på förhand vet att endast ett fåtal respektive en större krets kommer att behandla uppgifterna. Även i de fall där detta inte står klart från början kan man oftast av arbetsuppgiftens

art och storlek sluta sig till om uppgifterna sannolikt kommer att behandlas av ett fåtal tjänstemän eller av en större krets.

I viss utsträckning kan också tidsaspekten ha betydelse för om uppgifter ska anses vara gemensamt tillgängliga eller inte. Detta har, som *Riksdagens ombudsmän* påpekar, att göra med att uppgifter som behandlas under en längre tid typiskt sett kommer fler till del, t.ex. därför att personer i en från början begränsad krets med tiden byts ut. Viss brottsbekämpande verksamhet, främst underrättelseverksamhet, leder inte alltid till ett bestämt avslut av ett visst konkret ärende. Vissa underrättelseprojekt har t.ex. inte sällan obestämd varaktighet och kan därför komma att löpa över en längre tid. Som exempel kan nämnas projekt riktade mot ungdomsbrottsligheten på en viss ort eller underrättelseprojekt avseende viss typ av mc-brottslighet eller häleriverksamhet i en viss bransch. Det ligger i sakens natur att i sådana långvariga projekt kan den personal som sysslar med projektet komma att ersättas under arbetets gång. Även om tanken från början har varit att endast en liten avgränsad krets ska syssla med projektet, är det därför långtifrån alltid möjligt att upprätthålla det kravet. Uppgiftssamlingar som tas fram i ett sådant projekt, t.ex. en sammanställning över gängbrottsligheten på en viss ort, bör därför också anses som gemensamt tillgängliga personuppgifter.

Datainspektionen invänder mot de principer för gränsdragningen som promemorian föreslår och som i allt väsentligt läggs till grund för bedömningen här. Enligt regeringens mening skulle det bli för komplicerat för tillämparen att, som inspektionen förordar, utforma en lagregel där även antalet uppgifter och deras struktur vägs in i bedömningen och där bestämmelserna om gemensamt tillgängliga uppgifter görs tillämpliga på all insamling av uppgifter som är avsedda att göras gemensamt tillgängliga eller som kan antas komma att bli det. Flera remissinstanser framhåller just vikten av så klara riktlinjer som möjligt för gränsdragningen mellan personuppgifter som är gemensamt tillgängliga och sådana som inte är det. Av nyss angivna skäl bör inte bestämmelserna om gemensamt tillgängliga uppgifter, som inspektionen föreslår, göras tillämpliga på all insamling av uppgifter som är avsedda att göras gemensamt tillgängliga eller som kan antas komma att bli det. Som framhålls i promemorian kan det vid sådan insamling dock vara värdefullt att beakta de regler som gäller för behandling av gemensamt tillgängliga uppgifter för att inte försvåra den fortsatta behandlingen. De risker från integritetsskyddssynpunkt som inspektionen befarar både vad gäller uppbyggnad av stora, strukturerade samlingar av personuppgifter och okontrollerad insamling av uppgifter med digital teknik får inte överdrivas. Det finns andra regler som styr polisens verksamhet och som motverkar sådana risker. Som exempel på sådana andra bestämmelser kan nämnas reglerna om förundersökning och användning av tvångsmedel. Regeringen delar inte heller inspektionens åsikt att de mer begränsande bestämmelserna om gemensamt tillgängliga uppgifter alltid bör tillämpas i kriminalunderrättelseverksamhet. Polisen bör även kunna bedriva sitt arbete med att förebygga, förhindra och upptäcka brottslig verksamhet med modern teknik utan att de mer begränsande bestämmelserna om gemensamt tillgängliga uppgifter alltid blir tillämpliga, genom att t.ex. ta emot tips, använda e-post och ordbehandlingsprogram. Denna fråga behandlas i avsnitt 7.1 och 7.2. I avsnitt 9.2 redogörs för vilka uppgifter som bör få göras gemen-

samt tillgängliga i verksamhet som avser att förebygga, förhindra eller upptäcka brottslig verksamhet.

Polisen bör kunna samarbeta med andra brottsbekämpande myndigheter och inom ramen för sådant samarbete behandla personuppgifter i gemensamma projekt. Bland annat för att möjliggöra ett sådant samarbete görs bedömningen i avsnitt 12 att övriga brottsbekämpande myndigheter bör kunna beviljas direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga inom polisen. Syftet med att begränsa åtkomsten till gemensamt tillgängliga uppgifter är att personuppgifter – och behandlingen av sådana uppgifter – bör kringgärdas av ett extra skydd när de sprids till andra myndigheter än polisen. Konsekvensen av begränsningen blir, som *Kustbevakningen* och *Skatteverket* påpekar, att bestämmelserna om gemensamt tillgängliga uppgifter alltid blir tillämpliga i projekt med deltagare från andra myndigheter, oavsett antalet deltagare i projektet. Vad Kustbevakningen och Skatteverket anför i denna fråga föranleder inte någon annan bedömning än den som görs i promemorian. Kustbevakningens synpunkt att myndighetsövergripande projekt och aktioner bör kunna utföras med tillräckliga sökmöjligheter behandlas i avsnitt 11. I kommande avsnitt behandlas även *Rikspolisstyrelsens* invändning att vissa bestämmelser om sökbegränsningar och gallring som föreslås gälla för gemensamt tillgängliga uppgifter är för begränsande, se avsnitt 11 och 14.

Bestämmelserna om gemensamt tillgängliga uppgifter bör inte gälla för sådan behandling av personuppgifter som sker med stöd av bestämmelserna om diarieföring m.m. Skälen för detta redovisas i avsnitt 7.5.

Behovet av enhetlig tillämpning

Målsättningen är, som nyss nämnts, att här så tydligt som möjligt ange principerna för gränsdragningen mellan de personuppgifter som kan anses gemensamt tillgängliga och andra uppgifter. Någon formell gräns bör dock inte läggas fast i författning. För att uppnå enhetlighet i tillämpningen kommer det dock att finnas ett behov av ytterligare riktlinjer för polisens tillämpning av det nya begreppet. Det ankommer på Rikspolisstyrelsen att utforma de riktlinjer som behövs och att utbilda personalen.

9.2 Förebygga, förhindra eller upptäcka brottslig verksamhet

Regeringens förslag: I polisarbete som avser att förebygga, förhindra eller upptäcka brottslig verksamhet ska enbart följande personuppgifter få göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet som

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person som

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver och

b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

Tillgången till uppgifter om övervakning av en person ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning ska dock få göras tillgänglig för andra.

Utredningens förslag överensstämmer delvis med promemorians. Utredningen föreslår att bestämmelserna om kriminalunderrättelseverksamhet och kriminalunderrättelseregister ersätts med bestämmelser om behandling av uppgifter om andra personer än sådana som är misstänkta för brott. Enligt utredningen ska sådana uppgifter få behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Utredningen föreslår vidare att det under vissa förutsättningar ska vara tillåtet att behandla uppgifter, om det är nödvändigt för att underlätta övervakning av vissa grovt kriminellt belastade personer och personer som kan antas vara farliga. Utredningen föreslår inte att man ska skilja på gemensamt tillgängliga uppgifter och andra uppgifter.

Remissinstanserna: *Rikspolisstyrelsen* har uttalat att det bör vara tillräckligt att fängelse ingår i straffskalan för den misstänkta brottsliga verksamheten för att personuppgifter ska få behandlas. *Riksdagens ombudsmän* har ifrågasatt om nyttan med en bestämmelse som möjliggör registrering av uppgifter om övervakade personer väger över intresset av att skydda den enskilde mot integritetsintrång. *Justitiekanslern* har ansett att utformningen av bestämmelsen bör övervägas närmare och att en närmare precisering krävs av när en registrering får göras. Dåvarande *Riksåklagaren* har ansett att den tillåtna behandlingen bör begränsas till att avse personer som har dömts för allvarliga brott riktade mot en persons liv, hälsa eller frihet.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna har inget att invända mot promemorians förslag. *Riksdagens ombudsmän* anser dock att den nuvarande kvalifikationsgränsen om två års fängelse i straffskalan bör behållas för behandling av personuppgifter om misstänkt brottslig verksamhet. *Tullverket* däremot ställer sig bakom en ändring från två till

ett års fängelse. *Kammarrätten i Stockholm* uppger att domstolen i sak ställer sig bakom de preciseringar som föreslås gälla för uppgifter som ska få göras gemensamt tillgängliga men anser att rekvisitet ”sker systematiskt” bör analyseras närmare alternativt belysas ytterligare i författningskommentaren. *Datainspektionen* anser att det finns ett stort behov av att reformera bestämmelserna om kriminalunderrättelseverksamhet. Inspektionen anser sig dock inte på det underlag som finns kunna göra en nödvändig proportionalitetsbedömning och avstyrker därför förslaget (se även avsnitt 7.2).

I fråga om behandling av uppgifter för övervakning av personer anser *Riksdagens ombudsmän* att avgränsningen av vem som ska kunna anses vara allvarligt kriminellt belastad eller farlig för annans säkerhet måste göras såväl klarare som snävare. *Datainspektionen* saknar en närmare redogörelse för vilken eller vilka verksamheter som avses med övervakning av personer och lagstödet för denna verksamhet. Inspektionen anser vidare att det är oklart vilka ytterligare möjligheter till behandling av personuppgifter som de aktuella bestämmelserna är tänkta att ge stöd för. Inspektionen efterlyser ytterligare överväganden i fråga om innebörden och behovet av bestämmelserna.

Skälen för regeringens förslag

Den brottsliga verksamheten måste vara av allvarligare slag

Behandling av gemensamt tillgängliga uppgifter medför särskilda risker för intrång i den enskildes personliga integritet. Det är därför av vikt att möjligheterna att göra personuppgifter gemensamt tillgängliga begränsas till de situationer där behovet är påtagligt.

I avsnitt 7.2 beskrivs den verksamhet som omfattas av ändamålen förebygga, förhindra eller upptäcka brottslig verksamhet. Eftersom dessa begrepp, som *Kammarrätten i Stockholm* påpekar, är relativt vaga krävs det begränsningar i fråga om vilka uppgifter som ska få göras gemensamt tillgängliga. I det följande kommer för enkelhetens skull uttrycket underrättelseverksamhet att användas för att beskriva all den verksamhet som inryms i aktuella ändamål.

En första fråga är om den brottsliga verksamhet som underrättelsearbetet avser måste vara av allvarligare slag för att personuppgifter ska få göras gemensamt tillgängliga. Polisdatautredningen föreslår i denna del att det ska vara fråga om brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Det motsvarar vad som nu gäller för behandling av uppgifter i kriminalunderrättelseregister. I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet uppställs ett liknande krav. Enligt den lagen får uppgifter behandlas om de ger anledning att anta att verksamhet som innefattar brott för vilket är föreskrivet fängelse i minst två år eller brott som sker systematiskt har utövats eller kan komma att utövas (12 § första stycket 1). I sitt remissyttrande över Polisdatautredningens förslag framhöll *Rikspolisstyrelsen* att en sådan bestämmelse skulle medföra alltför stora begränsningar i förhållande till polisens behov av att kunna behandla personuppgifter. Styrelsen förordade i stället att personuppgiftsbehandling bör tillåtas om det finns fängelse i straffskalan för det brott som innefattas i den miss-

tänkta brottsliga verksamheten. Promemorian föreslår en lösning som ligger mellan Polisdatautredningens förslag och Rikspolisstyrelsens remissynpunkter. Promemorian ställer krav på misstänkt brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller mer. *Riksdagens ombudsmän* anser att en kvalifikationsgräns om två års fängelse torde ge ett tillräckligt utrymme för behandling av personuppgifter i polisens underrättelsearbete, bl.a. med hänsyn till den behandling som inryms i det i promemorian föreslagna undantaget för systematisk brottslig verksamhet.

Att tillåta att personuppgifter i underrättelseverksamhet i större utsträckning än vad som nu är fallet görs gemensamt tillgängliga kan framstå som betänkligt från integritetsskyddssynpunkt. Det förhållandet att uppgifter om brottslig verksamhet normalt har mindre konkretion än uppgifter om enskilda brott talar också för att polisen bör ges mindre utrymme för behandling av personuppgifter i underrättelseverksamhet än för behandling i t.ex. förundersökningar. Behovet av att behandla personuppgifter i underrättelseverksamhet framstår i allmänhet som mindre ju lägre straffvärde den brottsliga verksamhet har som underrättelseverksamheten avser. Det innebär emellertid inte att den nuvarande avgränsningen för när sådan behandling är tillåten – brottslig verksamhet som innefattar brott med minst två års fängelse i straffskalan – är den lämpligaste. Den nuvarande avgränsningen måste ses mot bakgrund av att underrättelseverksamhet var ett ganska nytt arbetssätt när polisdatalagen tillkom och att det då var naturligt att sätta upp förhållandevis snäva gränser för den behandling av personuppgifter som tilläts. Som redovisas i avsnitt 7.2 har polisens arbete med att förebygga, förhindra och upptäcka brottslig verksamhet utvecklats och den nuvarande avgränsningen av när personuppgifter får behandlas har med tiden visat sig vara en hämmande faktor i polisarbetet. Det är därför nödvändigt att i den nya lagen ge större utrymme än tidigare för behandling av uppgifter i verksamhet som bedrivs inom ramen för dessa ändamål.

I linje med vad Rikspolisstyrelsen förordat i sitt tidigare remissvar skulle man i och för sig kunna tänka sig att – i fråga om underrättelseverksamhet – tillåta att personuppgifter görs gemensamt tillgängliga så snart den brottsliga verksamheten innefattar brott för vilket fängelse ingår i straffskalan. En sådan reglering skulle dock föra alltför långt, eftersom många brott med fängelse i straffskalan normalt endast leder till bötesstraff.

Ett annat alternativ är att välja den lösning som promemorian föreslår nämligen att liksom hittills anknyta till straffskalan för de brott som den misstänkta verksamheten antas innefatta, men dra gränsen vid ett i stället för två års fängelse.

Promemorians förslag innebär bl.a. att polisen får större möjlighet att behandla personuppgifter i underrättelseverksamhet angående brott som regleras inom specialstraffrätten. Av tradition har många sådana brott en annan straffskala än brottsbalksbrott. Samtidigt är det fråga om brott som kan drabba enskilda brottsoffer mycket hårt och som av det skälet bör kunna beivras effektivare. Ett exempel på sådan brottslighet är s.k. inkassoverksamhet som bedrivs utan tillstånd. Det är en brottstyp som förekommer allt oftare och som förknippas med organiserad brottslighet, främst s.k. mc-brottslighet. Brotten består i att driva in pengar under

förtäckta hot. Även i de fall där brotten rubriceras som olaga hot är straffmaximum ett års fängelse. En annan brottstyp där det också kan vara angeläget att kunna samla och på ett mer kvalificerat sätt behandla underrättelseinformation för att kunna förebygga brott är överträdelse av besöksförbud. Även bland brottsbalksbrotten finns det sådana som bör kunna angripas genom en effektiv underrättelseverksamhet, men som med dagens gränsdragning faller utanför möjligheterna till behandling av personuppgifter, t.ex. skadegörelse i form av klotter. Denna brottstyp begås av ett fåtal personer men vållar stor skada för samhället. För att kunna lagföra klottrare krävs det normalt att de ertappas på bar gärning, vilket många gånger förutsätter ett noggrant underrättelsearbete. Andra brottsbalksbrott som i vissa fall kan kräva ett effektivt underrättelsearbete är skyddande av brottsling och främjande av flykt. Detta gäller särskilt i de fall där det finns misstanke om kommande fritagning av allvarligt brottsbelastade personer.

I sammanhanget är det viktigt att betona att en stor del av polisens behandling av personuppgifter i underrättelseverksamhet kommer att omfattas av de mer begränsande bestämmelserna om gemensamt tillgängliga uppgifter. Brottsförebyggande arbete i projektform där antalet deltagare är fler än ett tiotal omfattas exempelvis av dessa bestämmelser. Polisen bör enligt regeringens mening kunna bedriva underrättelsearbete för att stävja även mindre allvarlig brottslig verksamhet, bl.a. sådan verksamhet som innefattar brott av de slag som nyss angetts. Av betydelse från integritetsskyddssynpunkt är att ju mindre allvarlig brottslig verksamhet det är fråga om desto mindre är som regel behovet av att sprida uppgifter. Polisen ansvarar för att tillgången till uppgifter begränsas till den personal som behöver ha tillgång till dem för att kunna utföra sina arbetsuppgifter.

Sammanfattningsvis bör det enligt regeringens mening i verksamhet för att förebygga, förhindra och upptäcka brott vara möjligt att göra uppgifter gemensamt tillgängliga så snart den brottsliga verksamheten innefattar brott med ett års fängelse i straffskalan.

Det förekommer även brottslighet där ett års fängelse inte ingår i straffskalan för det enskilda brottet, men där verksamheten kan misstänkas ske systematiskt. Det kan exempelvis vara fråga om ligor som har satt i system att begå snatterier. Andra exempel finns inom den ekonomiska brottsligheten, där bl.a. osant intygande, som inte är grovt, utgör ett betydande problem och där brottsligheten ofta bedrivs systematiskt och kan kräva kartläggning. Ett tredje exempel är barnpornografibrott som är ringa. Intresset av en effektiv brottsbekämpning talar för att polisen bör kunna göra även uppgifter med anknytning till sådan systematisk brottslighet gemensamt tillgängliga. En motsvarande ordning gäller för närvarande för Tullverket. Bestämmelser som gör det möjligt att göra också personuppgifter, som har samband med misstänkt brottslig verksamhet som sker systematiskt, gemensamt tillgängliga bör därför införas i den nya lagen.

Polisens underrättelsearbete avseende mindre allvarlig brottslighet kommer, som Riksdagens ombudsmän påpekar, sannolikt att avse främst systematisk brottslig verksamhet. Det finns emellertid behov av att kunna göra uppgifter gemensamt tillgängliga även beträffande brottslig verksamhet som innefattar brott med endast ett år i straffskalan och som inte bedrivs systematiskt. En sådan behandling är ofta en förutsättning för att

polisen ska kunna se samband och upptäcka att viss verksamhet bedrivs systematiskt.

Uppgifterna måste antas ha samband med den brottsliga verksamheten

En annan fråga är *vilka* personuppgifter som bör få göras gemensamt tillgängliga och därefter behandlas gemensamt. Det är en självklarhet att uppgifter om brottsmisstankar och om de personer som är misstänkta för delaktighet i brottslig verksamhet ska få behandlas. Även uppgifter om den som inte kan misstänkas måste emellertid kunna få behandlas. Som exempel kan nämnas uppgifter om den som har informerat polisen om den misstänkta brottsliga verksamheten, uppgifter om en person som äger ett garage eller annan lokal där den misstänkta brottsliga verksamheten bedrivs och uppgifter om anhöriga eller andra som genom sitt samröre med den misstänkte kan vara av intresse i underrättelsearbetet. Som förutsättning för att uppgifter av detta slag ska få behandlas bör dock gälla att uppgifterna har en koppling till misstänkt brottslig verksamhet. Därför föreslås att bara uppgifter som kan antas ha samband med den misstänkta brottsliga verksamheten får behandlas.

Förslaget innebär att det i vissa fall kommer att vara möjligt att göra uppgifter om personer som inte själva är misstänkta för vare sig ett konkret brott eller för att delta i viss brottslig verksamhet gemensamt tillgängliga. Att sådan behandling bör omgärdas av särskilda bestämmelser till skydd för den enskildes integritet är självklart. Det behövs bl.a. bestämmelser som förhindrar att uppgifterna ges omotiverad spridning.

Frågan är då hur sådana skyddsregler lämpligen bör utformas. I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns bestämmelser som anger att personuppgifter av det nu diskuterade slaget får behandlas endast i ett ärende som rör viss preciserad brottslig verksamhet. Vidare får endast de som arbetar med ärendet ha direkt tillgång till uppgifterna. *Tullverket* lyfter fram just dessa bestämmelser som exempel på att dess lagstiftning är utformad så att den begränsar utrymmet för informationsutbyte och att detta försvårar samverkan mellan de brottsbekämpande myndigheterna.

Begränsningar av detta slag framstår som mindre ändamålsenliga för polisens del, särskilt mot bakgrund av Tullverkets erfarenheter. De skulle i alltför hög grad begränsa polisens möjlighet att förebygga, förhindra och upptäcka brottslig verksamhet. Det är inte ovanligt att samma personer är inblandade i flera brottsliga aktiviteter som pågår i olika delar av landet vid en och samma tidpunkt. Om endast de som arbetar med det ärende där en viss uppgift har kommit fram ges tillgång till uppgiften, kommer det normalt inte att vara möjligt att upptäcka sambanden med brottsliga aktiviteter som bedrivs på andra håll. Sådana samband kan utgöra grunden för en brottsmisstanke mot en person som förekommer som ”kringperson” i flera utredningar om likartad brottslig verksamhet. Uppgifter om personer som har samband med brottslig verksamhet utan att vara misstänkta bör därför kunna behandlas gemensamt inom polisen även utanför ett visst ärende. De särskilda risker för intrång i den personliga integriteten som detta skulle kunna innebära kan motverkas genom bl.a. begränsningar i möjligheterna att genom sökning få fram vissa upp-

gifter. Den frågan behandlas i avsnitt 11. Dessutom bör det beträffande uppgifter som görs eller har gjorts gemensamt tillgängliga alltid framgå huruvida en person är misstänkt eller inte samt för vilket närmare ändamål som behandlingen sker, vilket utvecklas i avsnitt 10. Den allmänna bestämmelsen om att endast personer som behöver uppgifterna för sitt arbete får ges tillgång till dem har också stor betydelse (avsnitt 6.6).

Uppgifter som behövs för övervakningen av vissa personer

Både Polisdatautredningen och promemorian föreslår särskilda bestämmelser som klargör att polisen i vissa fall har rätt att behandla uppgifter för övervakning av personer. Det handlar då om övervakning av personer som är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

Även Registerutredningen föreslog sådana bestämmelser (SOU 1997:65 s. 230 f.). Enligt det förslaget skulle kriminalunderrättelseregister få innehålla uppgifter om dömda personer som antingen var allvarligt kriminellt belastade eller som kunde antas vara farliga för annans personliga säkerhet. Personuppgifterna skulle gallras senast när samtliga uppgifter om personen hade gallrats ur belastningsregistret. Den dåvarande regeringen ansåg dock att några sådana bestämmelser inte borde införas (prop. 1997/98:97 s. 113 f.). Som skäl angavs att det var svårt att se något behov av ett sådant register, varvid det bl.a. hänvisades till registreringen i belastningsregistret. Regeringen menade också att det skulle vara svårt att fastställa vilka kriterier som skulle gälla för att en person skulle anses vara allvarligt kriminellt belastad eller farlig för annans säkerhet.

Tidigare utredningar och promemorian anser det befogat att polisen, under vissa förutsättningar, genom behandling av personuppgifter får möjlighet att utöva särskild kontroll över personer som är allvarligt kriminellt belastade eller som har visat sig vara särskilt farliga för andra personers säkerhet. Regeringen anser att sådan övervakning kan utgöra ett betydelsefullt inslag i polisens samlade insatser för att förebygga, förhindra eller upptäcka brottslig verksamhet. De uppgifter som finns i misstanke- och belastningsregistren ger inte all den information som behövs för en ändamålsenlig övervakning och registren innehåller inte heller de analysverktyg som kan krävas för att övervakningen ska bli effektiv.

Det förekommer redan övervakning av detta slag inom ramen för särskilda undersökningar. Med hjälp av ett särskilt analysverktyg kan informationen analyseras och kopplingar mellan exempelvis olika grupperingar, händelser och brottsliga verksamheter upptäckas. Denna form av uppgiftssamling har i något fall benämnts Y-databas, där bokstaven Y står för yrkeskriminell. Datainspektionen har i ett tillsynsärende inspekterat behandlingen av personuppgifter i en sådan databas vid Polismyndigheten i Skåne. Efter att inledningsvis ha ifrågasatt om databasen omfattades av polisdatalagens bestämmelser om särskilda undersökningar, kom inspektionen fram till att så var fallet. Inspektionen framförde dock vissa synpunkter på gallringen av uppgifterna (Datainspektionens beslut den 25 maj 2007, dnr 686-2006).

Datainspektionen har efterlyst klargöranden av vilken verksamhet som avses med begreppet övervakning. Vad som avses är just den nyss beskrivna behandlingen i form av lagring, bearbetning och analys som sker i särskilda uppgiftssamlingar för att utöva kontroll över vissa personer som uppfattas som särskilt brottsbenägna eller farliga, men mot vilka det för tillfället inte finns några konkreta misstankar om brottslig verksamhet.

Uppgiftssamlingar av detta slag är av stor betydelse för att polisen långsiktigt ska kunna bedriva ett effektivt brottsbekämpande arbete. Utan tillgång till sådana uppgiftssamlingar skulle det vara svårt för polisen att bemästra den brottslighet som förekommer i kriminella nätverk som exempelvis mc-brottsligheten. Från integritetssynpunkt är i och för sig personuppgiftsbehandling av detta slag ägnad att inge betänkligheter. Detta intrång måste dock ställas mot behovet av att förebygga brott av allvarligt slag.

Frågan är då i vilken utsträckning den nya lagen bör ge polisen möjlighet att skapa sådana gemensamma uppgiftssamlingar. För att det integritetsintrång som personuppgiftsbehandlingen kan ge upphov till inte ska bli oproportionerligt bör möjligheten till behandling av personuppgifter för övervakning inskränkas till att avse uppgifter om och kring de personer som uppfattas som särskilt brottsaktiva eller farliga. Bestämmelsen bör dock utformas något annorlunda än vad som föreslås i promemorian. Som första förutsättning bör gälla att personen kan antas komma att begå brott av mera allvarligt slag; att han eller hon tidigare är dömd för sådana brott bör alltså inte vara tillräckligt. Med brott av mera allvarligt slag avses här brott med fängelse i två år eller mer i straffskalan. Därutöver bör krävas att personen antingen är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

Riksdagens ombudsmän anser att avgränsningen av vem som ska kunna anses vara allvarligt kriminellt belastad eller farlig för annans säkerhet måste göras såväl klarare som snävare. Varken Polisdatautredningen, Registerutredningen eller promemorian anser dock att det är ändamålsenligt att i lagtext närmare precisera uttrycken ”allvarlig kriminell belastning” och ”hot mot andras säkerhet”. Innebörden i dessa begrepp kommer att behandlas närmare i författningskommentaren. Någon precisering utöver vad som sägs där kan inte anses nödvändig. Både dåvarande *Riksåklagaren* och *Riksdagens ombudsmän* anger som möjlig avgränsning att endast tillåta övervakning av personer som dömts för allvarliga brott riktade mot annans liv, hälsa eller frihet. Detta skulle dock enligt regeringens mening bli för begränsande, eftersom flera av de personer som polisen tror sig veta livnär sig på allvarlig brottslighet aldrig har dömts för något sådant brott. Vidare bör vissa brott som inte direkt kan anses riktade mot liv, hälsa eller frihet kunna omfattas, exempelvis grova skattebrott och narkotikabrott. Sådana brott är nämligen ofta led i grov organiserad brottslighet riktad mot liv, hälsa eller frihet, t.ex. människohandel.

För att en bestämmelse av detta slag ska bli meningsfull bör polisens möjlighet att göra uppgifter gemensamt tillgängliga omfatta inte bara uppgifter som direkt avser de övervakade personerna utan även uppgifter om personer som har samband med de övervakade personerna. Uppgifter måste exempelvis kunna behandlas om att en övervakad person är an-

ställd hos en viss annan person och att den övervakade personen regelbundet besöker vissa personer. En förutsättning för behandlingen bör dock vara att uppgiften behövs för övervakningen.

Som *Datainspektionen* påpekar torde personuppgiftsbehandling av nu aktuellt slag för att möjliggöra övervakning i många fall rymmas inom de allmänna bestämmelserna om när uppgifter får göras gemensamt tillgängliga i underrättelsearbete. De uppgifter som behöver behandlas för övervakningen kommer med stor sannolikhet att ofta ha samband med misstänkt brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver eller som sker systematiskt. Det kan dock förekomma fall där dessa rekvisit inte är uppfyllda, samtidigt som starka skäl talar för att behandling bör kunna ske. Det kan exempelvis ibland vara svårt att precisera misstänkt brottslig verksamhet. Vidare – vilket är den största skillnaden – kan uppgifter om personer som har koppling till den övervakade behandlas i större utsträckning eftersom det inte ställs något krav på samband med brottslig verksamhet.

Tillgången till de behandlade uppgifterna bör liksom nu vara starkt begränsad. Endast de tjänstemän som har till uppgift att arbeta med övervakningen bör kunna medges åtkomst. Information om att en viss person är föremål för övervakning bör dock kunna spridas till flera, eftersom det kan vara en förutsättning för att övervakningen ska bli effektiv. Det bör tydligt framgå att personuppgifter behandlas för att möjliggöra övervakning (se avsnitt 10).

9.3 Utreda och beivra brott

Regeringens förslag: Personuppgifter i ärenden om utredning eller beivrande av brott ska få göras gemensamt tillgängliga.

Utredningen föreslår inte att man ska skilja på uppgifter som är gemensamt tillgängliga och andra uppgifter.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag: Det är självklart att uppgifter som behandlas för att utreda och beivra brott måste kunna göras gemensamt tillgängliga för de tjänstemän som arbetar med utredningen. Att sådana uppgifter kan göras gemensamt tillgängliga är också en förutsättning för att direktåtkomst ska kunna ges till åklagare, som ofta leder förundersökningar. Det finns inte anledning att ställa upp något krav på att det ska vara fråga om utredning av allvarligare brott för att sådan behandling ska vara tillåten. Flertalet förundersökningar, oavsett misstänkt brott, lagras redan nu i digital form i ett särskilt system kallat Datoriserad utredningsrutin (DurTvå; se *bilaga 6*).

Av lagen bör det således framgå att samtliga uppgifter som förekommer i ett ärende som avser utredning eller beivrande av brott får göras gemensamt tillgängliga. Det bör dock göras ett undantag från denna

huvudregel, nämligen när det gäller DNA-profiler. Den frågan behandlas i avsnitt 9.6.

I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet föreskrivs som huvudregel att endast de personer som arbetar med ett ärende får ha direkt tillgång till uppgifter som behandlas i ärendet. En följd av detta är att möjligheten att utnyttja uppgifter som behandlas inom ramen för en utredning i en annan utredning eller i underrättelseverksamhet försvåras. Det är inte rimligt att ställa upp någon motsvarande begränsning för polisen. I en brottsutredning kan det vara viktigt att uppgifter snabbt kan inhämtas från andra brottsutredningar, så att polisen kan bedöma om det finns några samband mellan utredningarna. Uppgifter i en förundersökning måste således kunna göras gemensamt tillgängliga för andra än de som arbetar i förundersökningen. Uppgifter av detta slag är redan nu i viss utsträckning gemensamt tillgängliga. Tillgången till uppgifter i systemet DurTvå är nämligen inte begränsad till de personer som arbetar med en viss förundersökning. För närvarande registreras även samtliga brottsanmälningar i systemet Rationell anmälningsrutin (RAR; se *bilaga 6*). Samtliga personuppgifter läggs in i systemet, men endast vissa uppgifter får göras sökbara. Från RAR och DurTvå hämtas uppgifter till andra register, t.ex. till det centrala brottsspaningsregistret som innehåller uppgifter om anmälda brott, tillvägagångssätt, signalement beträffande personer som setts på brottsplatsen m.m. Uppgifter från förundersökningar hämtas också till andra register. Att uppgifter i en brottsanmälan eller en förundersökning görs tillgängliga inom polisen för andra än de som arbetar i ärendet är alltså något som redan nu förekommer i stor utsträckning och är en förutsättning för ett effektivt polisarbete. I de flesta fall är det endast fråga om att göra vissa typer av uppgifter tillgängliga för andra än de som arbetar i förundersökningen, inte hela förundersökningen.

Det förhållandet att det öppnas möjlighet att göra uppgifter om utredning av brott gemensamt tillgängliga innebär naturligtvis inte någon skyldighet att göra det. Uppgifter i vissa förundersökningar av särskilt känsligt slag bör sannolikt överhuvudtaget inte göras tillgängliga för andra än de som arbetar med förundersökningen. I vilken utsträckning möjligheten bör utnyttjas bör dock överlämnas till polisen att avgöra i det enskilda fallet.

Det bör anmärkas att Åklagardatautredningen i betänkandet med förslag till lag om behandling av uppgifter i åklagarväsendets brottsbekämpande verksamhet inte föreslår några begränsningar i fråga om möjligheten att göra uppgifter som förekommer i ärenden om utredning eller beivrande av brott gemensamt tillgängliga (SOU 2008:87 s. 227).

9.4 Uppgifter som rapporteras till polisens kommunikationscentraler

Regeringens förslag: Uppgifter som rapporteras till polisens kommunikationscentraler ska få göras gemensamt tillgängliga i polisens brottsbekämpande verksamhet.

Utredningen behandlar inte frågan.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag: Polisens kommunikationscentraler har till uppgift att effektivisera och samordna bl.a. de åtgärder som larm föranleder. Kommunikationscentralerna tar emot och vidarebefordrar inkommande larm och andra meddelanden samt vidtar och samordnar inledningsvis polisåtgärder med anledning av larm. Som stöd för denna verksamhet finns ett särskilt datasystem för kommunikationscentralerna, det s.k. KC-systemet (se *bilaga 6)*. Till kommunikationscentralerna rapporterar polispersonalen in händelser, iakttagelser och utförda uppdrag. KC-systemet syftar till att dokumentera, bevaka och följa upp händelser och iakttagelser som rapporteras till kommunikationscentralerna både av allmänheten och av polispersonal. Syftet är också att på ett tidigt stadium kunna få signaler om pågående och återkommande brottslighet. Vidare har behandlingen till ändamål att ge underlag för planering av polisens resurser och för uppföljning av verksamheten. Systemet stöder inte endast polisens brottsbekämpande verksamhet utan även annan polisiär verksamhet. Uppgifterna som antecknas i systemet får vara tillgängliga i tretton månader.

När kommunikationscentralen tar emot larm och meddelanden, antecknas den information som rapporteras in. Vidare antecknas vilka åtgärder som vidtas med anledning av ett larm, t.ex. om en polispatrull skickas till platsen där ett brott påstås ha begåtts. När polispatrullen har varit på platsen, rapporterar den till kommunikationscentralen vad som har hänt och vilka ytterligare åtgärder som bedöms vara nödvändiga. Det finns inte några begränsningar i fråga om vilka uppgifter som får antecknas i KC-systemet. Det som registreras är bl.a. brotts- eller händelseplatser med besked om tid, plats, händelsetyp, brottskod och övrig information som kan vara till hjälp vid en kommande insats. Systemet innehåller också personuppgifter. Något förenklat kan man säga att systemet fungerar som en postcentral där alla inrapporterade uppgifter antecknas för att senare sorteras och vidarebefordras till polisens olika verksamhetsgrenar. Uppgifter om misstänkta brott vidarebefordras till polisens utredningsenheter, medan uppgifter om misstänkt brottslig verksamhet förs över till polisens underrättelseenheter. KC-systemet används normalt inte i den brottsbekämpande verksamheten för att söka efter information. Det förekommer emellertid att sökningar görs i systemet för att få fram uppgifter till en pågående brottsutredning, t.ex. om vad som har rapporterats in till polisen under en viss kortare tidsperiod eller på en viss plats. Det är dock endast ett begränsat antal tjänstemän som har behörighet att söka i systemet.

Polisen bör även fortsättningsvis ha möjlighet att dokumentera händelser och iakttagelser som rapporteras till polisens kommunikationscentraler. För att en sådan dokumentation ska tillgodose polisens informationsbehov är det nödvändigt att uppgifterna kan göras gemensamt tillgängliga. Som framgått ovan kan det som rapporteras innehålla vilka personuppgifter som helst. Meddelandena kan således mycket väl innehålla uppgifter som inte annars får göras gemensamt tillgängliga enligt

de bestämmelser som föreslås i den nya lagen. Det kan t.ex. röra sig om uppgifter om personer som enbart misstänks delta i brottslig verksamhet som inte innefattar brott för vilket är föreskrivet ett års fängelse eller mer. Att i detta sammanhang göra skillnad på den ena eller andra typen av uppgifter är dock praktiskt ogörligt. Den personal som tar emot och dokumenterar uppgifterna har inte någon möjlighet att pröva hur uppgifterna får behandlas.

Mot denna bakgrund bör det i den nya lagen tas in en särskild bestämmelse som ger ett generellt stöd för den behandling av personuppgifter som sker vid polisens kommunikationscentraler. Uppgifterna bör få göras gemensamt tillgängliga i polisens brottsbekämpande verksamhet.

Det ska tydligt framgå att personuppgifter behandlas för nu aktuellt ändamål genom en särskild upplysning eller på något annat sätt. Vidare bör särskilda gallringsbestämmelser gälla. Dessa frågor behandlas i avsnitt 10 och 14.3.

9.5 Uppgifter i det internationella samarbetet

Regeringens förslag: Uppgifter i det internationella samarbetet får göras gemensamt tillgängliga om det behövs för att fullgöra den aktuella förpliktelsen.

Utredningen behandlar inte frågan.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Rikspolisstyrelsen* ifrågasätter dock om inte kravet på att uppgifterna ska behövas för att fullgöra en internationell förpliktelse redan framgår av den bestämmelse som anger att endast uppgifter som behövs för att fullgöra en internationell förpliktelse får göras gemensamt tillgängliga.

Skälen för regeringens förslag: Den ökade internationaliseringen innebär att allt större krav ställs på polisiärt samarbete över gränserna (se avsnitt 7.4). Den föreslagna lagen bör därför ge möjlighet till personuppgiftsbehandling för internationellt samarbete. En grundläggande förutsättning för sådan behandling bör vara att den behövs för att fullgöra ett internationellt åtagande. En särskild fråga är hur man ska se på möjligheten att göra uppgifter gemensamt tillgängliga när det gäller internationellt samarbete. I princip bör man kunna utgå från samma kriterier i det arbetet som vid personuppgiftsbehandling för nationella behov.

En viktig del av det dagliga internationella samarbetet via Interpol består i utbyte av information om stulna pass, stulna fordon, stulen konst och efterlysta personer. Interpol för olika register över sådana uppgifter och medlemsstaterna utbyter fortlöpande denna information med varandra. Syftet med s.k. internationell efterlysning av personer eller föremål är att man genom det förfarandet förbättrar möjligheterna att utreda och lagföra brott. Informationsutbytet ökar möjligheterna att påträffa

personer som försöker hålla sig undan rättvisan. Likaså förbättras förutsättningarna för att kunna återställa stulen egendom eller att åtminstone förhindra att värdefulla stulna föremål avyttras i andra länder.

När en svensk myndighet sänder en internationell efterlysning till Interpol sker detta som ett led i den svenska brottsbekämpningen. Uppgifterna har då gjorts gemensamt tillgängliga med stöd av de regler som föreslås i avsnitt 9.2 och 9.3. När en svensk myndighet tar emot uppgifter från andra länder om internationella efterlysningar görs det för att den andra staten vill ha bistånd med upplysningar om var det efterlysta föremålet finns (och eventuellt med ett ingripande i form av beslag) eller hjälp med att ingripa mot den efterlysta personen, om denne påträffas i Sverige. Upplysningar om efterlysta personer och efterlysta föremål måste därför kunna vidarebefordras till i princip all polispersonal. Detta görs genom att uppgifterna tillförs de nationella registren över efterlysningar. För att svensk polis ska kunna fullgöra gjorda internationella åtaganden i nu aktuella hänseenden måste således personuppgifter i viss utsträckning kunna göras gemensamt tillgängliga.

Ett annat exempel där det kan krävas att uppgifter görs gemensamt tillgängliga är förundersökningar som bedrivs parallellt i Sverige och i en annan stat och som gäller brott och brottsmisstankar som har samband med varandra. Även underrättelseuppgifter som lämnas till Sverige som ett led i ett allmänt informationsutbyte kan behöva behandlas gemensamt för att den svenska polisen ska kunna bidra med information.

Den nya lagen bör alltså ge utrymme för att göra uppgifter som behandlas inom ramen för internationellt samarbete gemensamt tillgängliga. Mot bakgrund av de särskilda risker för intrång i den enskildes personliga integritet som behandling av gemensamt tillgängliga uppgifter kan medföra bör behandlingen begränsas till de fall där behovet är mera påtagligt. När det gäller personuppgifter som behandlas för att fullgöra internationella åtaganden bör därför dessa få göras gemensamt tillgängliga endast om det krävs för att förpliktelsen ska kunna fullgöras.

En uttrycklig bestämmelse om detta bör tas in i den nya lagen. Bestämmelsen bör dock utformas något annorlunda än promemorians förslag, för att undanröja den oklarhet som *Rikspolisstyrelsen* pekar på.

Den internationella enheten vid Rikskriminalpolisen fungerar som kontaktpunkt vid allt internationellt polisiärt samarbete som inte sker genom direktkontakter mellan myndigheterna. I avsnitt 15.5 diskuteras de särskilda behov av behandling av uppgifter som finns i det arbetet, vilket utmynnar i förslag att Rikspolisstyrelsen får föra ett särskilt register över internationella ärenden.

9.6 Behandlingen av DNA-profiler

Regeringens förslag: Uttrycket ”uppgifter om resultatet av DNA-analyser” ska ersättas med begreppet ”DNA-profil”.

DNA-profiler får inte göras gemensamt tillgängliga, men får behandlas i vissa register enligt särskilda bestämmelser. Utöver detta gäller inga särskilda begränsningar för behandlingen av DNA-profiler.

Utredningens förslag: Uppgifter om resultatet av DNA-analyser i brottmål ska endast få behandlas i särskilda register samt i förundersökningar och andra brottsutredningar.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer delvis med regeringens. Promemorian använder inte begreppet DNA-profil och föreslår att behandling av uppgifter om resultatet av DNA-analyser endast ska vara tillåten i förundersökningar, utöver den behandling som sker i de särskilda DNA-registren.

Remissinstanserna: Flertalet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Åklagarmyndigheten, Rikspolisstyrelsen* och *Statens kriminaltekniska laboratorium* ifrågasätter dock promemorians uttalande att DNA-profiler utgör särskilt känsliga uppgifter och framhåller att de DNA-profiler som tas fram och registreras i DNA-registren endast utgör en sifferkombination som inte innehåller någon information om personliga egenskaper, t.ex. sjukdomsanlag eller liknande. Mot denna bakgrund anser Åklagarmyndigheten att förnyade överväganden behövs vad gäller den föreslagna regleringen av behandling av DNA-profiler. Enligt Statens kriminaltekniska laboratorium är DNA-profiler inte mer integritetskänsliga än exempelvis fingeravtryck.

Rikspolisstyrelsen påpekar att DNA-profiler ofta utväxlas inom ramen för det internationella polisiära samarbetet. Bestämmelsen i förslaget med innebörd att DNA-profiler – utöver behandlingen i DNA-register – endast får behandlas i förundersökningar måste enligt styrelsen ändras för att det internationella uppgiftsutbytet ska kunna fortsätta. Styrelsen anser vidare att lagtexten bör förtydligas när det gäller uttrycket ”resultatet av DNA-analys”. Några remissinstanser ifrågasätter även att uppgifter om resultat av DNA-analyser inte ska få göras gemensamt tillgängliga. Statens kriminaltekniska laboratorium anser att lagtexten behöver förtydligas, bl.a. ifrågasätts hur bestämmelsen om undantag för möjligheten att göra DNA-profiler gemensamt tillgängliga förhåller sig till bestämmelserna om direktåtkomst till DNA-register.

Skälen för regeringens förslag: I polisdatalagen finns bestämmelser om behandlingen av uppgifter om resultatet av DNA-analyser. Sådana uppgifter får enligt 22 § behandlas i särskilda register samt i förundersökningar och i särskilda undersökningar. I promemorian föreslås en liknande reglering.

Som *Rikspolisstyrelsen* anför är uttrycket ”uppgifter om resultatet av DNA-analyser” otydligt och kan ge utrymme för olika tolkningar av vilken behandling som avses. I polisdatalagen används uttrycket ”uppgifter om resultatet av DNA-analyser” för att beskriva det som registreras i DNA-registren (registren beskrivs närmare i avsnitt 15.2). I departementspromemorian Genomförandet av delar av Prümrådsbeslutet beskrivs hur det går till när Statens kriminaltekniska laboratorium analyserar DNA-prov och tar fram DNA-profiler samt hur DNA-profilerna sedan används genom att jämföras med andra DNA-profiler (Ds 2009:8 s. 79 f.). Av redogörelsen framgår bl.a. följande. Vid en kriminalteknisk DNA-analys undersöks endast en liten del av arvsmassan med inriktning på olika analyser som benämns STR-områden. Typbestämningen av ett antal sådana STR-områden presenteras som en sifferkombination (DNA-profilen). Det är endast denna sifferkombination som registreras och

används för jämförelse med andra registreringar. Den del av DNA:t som typbestäms hör till den icke kodifierade delen av DNA:t. Det finns därför inga personliga egenskaper kopplade till dessa.

De uppgifter som får registreras efter en DNA-analys anges i 24, 24 a och 25 §§ polisdatalagen. Endast uppgifter som ger information om den registrerades identitet, samt uppgifter om vem analysen avser och i vilket ärende den gjorts får registreras. Det som läggs in i DNA-registren är således DNA-profilen och uppgifter om den undersöktes identitet, om den är känd, samt vissa administrativa uppgifter. För att tydliggöra att det är behandlingen av själva siffer- eller bokstavskombinationen som regleringen avser, och inte exempelvis behandlingen av ett utlåtande efter en företagen jämförelse av olika DNA-profiler, bör formuleringen ”uppgifter om resultat av DNA-analyser” ersättas med begreppet ”DNA-profil” . En definition av termen DNA-profil bör införas i den nya lagen. Av definitionen bör det framgå att en DNA-profil utgör resultatet av en DNA-analys som presenteras som en kombination av siffror eller bokstäver. Det bör också framgå att det är fråga om DNA-analys av humant material. Motsvarande ändringar har föreslagits i departementspromemorian Genomförandet av delar av Prümrådsbeslutet (Ds 2009:8 s. 120).

Några remissinstanser har kritiserat den föreslagna begränsningen att DNA-profiler endast ska få behandlas i förundersökningar och i särskilda register. Vid bedömningen av behovet av en sådan begränsning kan inledningsvis konstateras dels att det krävs expertkunskap för att tillgodogöra sig information ur en DNA-profil, eftersom en sådan profil endast utgör en kombination av siffror eller bokstäver, dels att den information som en expert kan ta fram ur en DNA-profil är begränsad. Detta innebär å ena sidan att det kan ifrågasättas om en DNA-profil utgör en sådan integritetskänslig uppgift som förutsätts i promemorian. Å andra sidan är det svårt att se något reellt polisärt behov av att kunna behandla DNA-profiler utanför den verksamhet som bedrivs av Statens kriminaltekniska laboratorium och utanför de särskilda register där DNA-profiler registreras. Som Rikspolisstyrelsen påtalar finns det dock ett sådant behov inom ramen för det internationella samarbetet, eftersom DNA-profiler redan nu i viss utsträckning utbyts med andra länder (se prop. 2007/08:83 s. 60). Att föreskriva att DNA-profiler endast får behandlas i förundersökningar är därför enligt regeringens mening inte lämpligt. Inte heller integritetsskyddsskäl motiverar en sådan begränsning. Det är viktigt att betona att den reglering som nu föreslås inte avser hanteringen av spårmaterialet eller DNA-proverna utan behandlingen av själva resultatet av analysen i form av en DNA-profil.

Däremot bör det införas ett förbud mot att göra DNA-profiler gemensamt tillgängliga. Denna begränsning är viktig av integritetsskyddsskäl, eftersom det därigenom bl.a. säkerställs att det inte skapas uppgiftssamlingar med DNA-profiler vid sidan av de särskilda register där DNA-profiler får behandlas.

Förbudet mot att göra DNA-profiler gemensamt tillgängliga torde inte, som *Rikspolisstyrelsen* befarar, utgöra något problem för det internationella uppgiftsutbytet eftersom det nu, till skillnad från i promemorian, föreslås särskilda bestämmelser för Rikspolisstyrelsens internationella register. I sammanhanget är det viktigt att framhålla, bl.a. med anledning av *Statens kriminaltekniska laboratoriums* begäran om förtydligande, att

förbudet mot att göra DNA-profiler gemensamt tillgängliga inte gäller behandlingen av uppgifter i de register som regleras särskilt.

I avsnitt 15.2 och 15.5 övervägs vilka bestämmelser som ska gälla för behandlingen av DNA-profiler i särskilda register.

10 Särskilda upplysningar för gemensamt tillgängliga uppgifter

Regeringens förslag: Vid behandling av gemensamt tillgängliga uppgifter ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål uppgifterna behandlas. Om en uppgift direkt kan hänföras till en person som inte är misstänkt vare sig för visst brott eller för att ha utövat eller komma att utöva allvarlig eller systematisk brottslig verksamhet, ska det på samma sätt framgå att personen i fråga inte är misstänkt.

Uppgifter, som avser en person som kan antas ha samband med misstänkt brottslig verksamhet, ska som regel förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detsamma gäller för personuppgifter som behandlas inom ramen för övervakning av brottsmisstänkta personer.

Utredningens förslag: Uppgifter om personer mot vilka det inte finns någon misstanke om brott ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Remissinstanserna har inte haft några invändningar mot utredningens förslag.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Åklagarmyndigheten* förklarar sig ha förståelse för de skäl som bär upp intresset av att ”märka” uppgifter med särskilda upplysningar. Myndigheten anser dock att det framstår som mycket svårt att praktiskt förverkliga en sådan ambition, inte minst vad gäller omfattande bild- och ljudmaterial.

Även *Rikspolisstyrelsen* förutser praktiska problem vid tillämpningen av de föreslagna bestämmelserna, framför allt i fråga om behandling av personuppgifter i form av bild och ljud. Styrelsen ifrågasätter exempelvis hur bestämmelserna om särskilda upplysningar ska kunna tillämpas vid videokonferenser för t.ex. utsättning i en myndighet. Styrelsen föreslår därför att behandling i form av bild och ljud undantas från kravet på särskilda upplysningar. Rikspolisstyrelsen anser vidare att det är svårt att förstå hur bestämmelserna ska tillämpas vid behandling av personuppgifter i löpande text och efterlyser därför klargöranden i den fortsatta beredningen. Förtydliganden behövs även i fråga om kravet på särskild upplysning om ändamålet med behandlingen. Rikspolisstyrelsen anser att bestämmelsen bör tolkas så att kravet är uppfyllt om uppgiften ingår i ett särskilt underrättelseprojekt eller särskilt system med visst ändamål eller om det finns information om hur uppgiften ska hanteras.

Rikspolisstyrelsen uppger att det i all underrättelseverksamhet finns ett verksamhetsbehov av att vid analys av information kunna bedöma källans tillförlitlighet och informationens riktighet i sak. Därför har polisen infört ett värderingssystem, det s.k. 4x4-systemet, som ska användas vid inhämtningen av information. Styrelsen bedömer att systemet i stort uppfyller förslagets krav på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Emellertid förekommer det enligt styrelsen att information som har inhämtats inte har åsatts någon värdering, t.ex. information som inhämtats från icke polisära källor och information som översänts från brottsbekämpande myndigheter i andra länder. Rikspolisstyrelsen föreslår därför att kravet modifieras genom att ange att uppgifter så långt som möjligt ska förses med särskild upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. I och med att äldre information inte alltid har åsatts en värdering är det enligt Rikspolisstyrelsen viktigt att bestämmelserna inte gäller retroaktivt. Den stora mängd information som finns i polisens system omöjliggör en retroaktiv tillämpning.

Skälen för regeringens förslag

Krav på att vissa förhållanden ska framgå

Traditionella register förs för vissa närmare preciserade ändamål. När personuppgifter lagras i ett sådant register framgår det således av sammanhanget för vilket ändamål uppgiften lagras. Eftersom register vanligtvis konstrueras så att sökfält skapas för olika slag av uppgifter får den som söker efter information i register normalt också upplysning om till vilken kategori en viss uppgift hör, t.ex. misstänkt eller målsägande. En utgångspunkt för arbetet med den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet är att lagen inte bör reglera hur uppgifter tekniskt ska lagras eller göras tillgängliga. Förslaget innebär att uppgifter av olika slag kan göras gemensamt tillgängliga utan att de för den skull behöver ingå i ett särskilt register av vilket de närmare ändamålen för behandlingen av personuppgifterna framgår. Uppgifter ska således i större utsträckning kunna lagras i det sammanhang som de lagligen samlades in för och därifrån göras tillgängliga för olika berättigade ändamål.

I och med att den nya lagen i större utsträckning kommer att tillåta att uppgifter behandlas utanför särskilda register behövs bestämmelser som säkerställer att den som söker information får motsvarande upplysningar, bl.a. om ändamålet för behandlingen, som han eller hon skulle ha fått om uppgifterna hade behandlats i ett register. Både verksamhetsskäl och integritetsskyddsskäl talar för att det vid informationssökning ska framgå varför en uppgift behandlas av polisen. Av samma skäl är det viktigt att det framgår att en uppgift rör en icke-misstänkt person när så är fallet samt hur tillförlitlig en underrättelseuppgift bedöms vara. Sådan information är nödvändig om en uppgift tas ur sitt sammanhang för att behandlas för ett nytt ändamål. Mot denna bakgrund bör det som promemorian föreslår införas krav på att vissa förhållanden alltid ska framgå. I förtydligande syfte bör bestämmelserna utformas på ett något annorlunda sätt än i promemorians förslag. Det bör föreskrivas att aktuellt förhål-

lande ska framgå genom en särskild upplysning eller på något annat sätt. Någon förändring i sak är dock inte avsedd utan utgångspunkten är densamma, nämligen att upplysning aldrig behöver lämnas om förhållande som ändå framgår av omständigheterna. Vad detta närmare innebär utvecklas i det följande.

I linje med utgångspunkten att några särskilda upplysningar inte behövs när det ändå framgår varför uppgiften behandlas, föreslås inte några motsvarande bestämmelser för uppgifter som ännu inte har gjorts gemensamt tillgängliga. Om t.ex. uppgifter förekommer i en enskild tjänstemans dator eller behandlas i en liten, klart avgränsad projektgrupp vet handläggande tjänsteman varifrån uppgiften har kommit, varför den behandlas och om en omnämnd person är misstänkt för brott eller för att utöva brottslig verksamhet eller inte.

I vilken utsträckning det kommer att bli nödvändigt att förse uppgifter med särskilda upplysningar beror på hur polisen organiserar behandlingen av personuppgifter i den brottsbekämpande verksamheten. När uppgifter behandlas i särskilda avgränsade register eller system framgår det normalt av omständigheterna för vilket ändamål uppgifterna behandlas och om en uppgift avser en person som är misstänkt eller inte. Förhållandena ändras om man bygger system som möjliggör sökning exempelvis på viss person i ett flertal system; flera olika särskilda undersökningar kanske länkas samman. I sådana fall är det viktigt att det framgår varifrån uppgiften hämtats, för vilket ändamål uppgiften behandlas och om uppgiften avser någon som inte är misstänkt.

Sammanfattningsvis bör framhållas att det väsentliga är att den som får del av personuppgifter inom polisen ska veta varför uppgifterna behandlas. I vilken utsträckning särskilda upplysningar kommer att behövas, blir avhängigt av vilka lösningar polisen väljer för sin framtida personuppgiftsbehandling. Behålls de traditionella registren kommer några särskilda upplysningar normalt inte att behövas, eftersom ändamålet med behandlingen då framgår av syftet med registret.

Uppgifter i bild- och ljudupptagningar m.m.

Både *Åklagarmyndigheten* och *Rikspolisstyrelsen* förutser praktiska problem vid tillämpningen av bestämmelserna om särskilda upplysningar. Båda myndigheterna pekar på särskilda svårigheter vid behandling av uppgifter i form av bild och ljud.

Bestämmelserna kan i förstone framstå som mer ingripande och begränsande än vad som är fallet. Det är bl.a. mot denna bakgrund som bestämmelserna föreslås utformas på ett något annorlunda sätt än i promemorieförslaget. Inledningsvis bör betonas att det inte ställs upp något krav på ”märkning” av varje enskild personuppgift i en bild- eller ljudupptagning. Det viktiga är att den som får tillgång till och söker i en bild- eller ljudfil vet varifrån upptagningen härrör och för vilket ändamål den behandlas. Det kan t.ex. uppnås genom att den aktuella filen förses med en särskild upplysning om ändamålet med behandlingen. Ibland behövs ingen upplysning; för exempelvis en upptagning vid hemlig kameraövervakning eller hemlig teleavlyssning i en förundersökning om grovt nar-

kotikabrott krävs inga ytterligare upplysningar om ändamålet med behandlingen.

Om det inte framgår av sammanhanget, kan det i anslutning till bild- eller ljudfilen även behövas en särskild upplysning, t.ex. i form av en förklarande text, om vilken eller vilka personer på upptagningen som är misstänkta för brott. Därmed framgår det motsatsvis att övriga personer inte är misstänkta. Det kan exempelvis behövas en särskild upplysning om det finns spaningsbilder från en viss plats där det förekommer flera personer och endast en av dem är misstänkt. I vissa fall behövs även en värdering av uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Rikspolisstyrelsen ifrågasätter även hur uppgifter ska kunna förses med särskilda upplysningar vid en videokonferens. Vid en sådan konferens är det vanligt att personuppgifter behandlas, eftersom syftet normalt är att utbyta information om personer. Vid s.k. utsättning diskuterar polisen olika händelser, företeelser och personer och det förekommer att bilder visas. Eftersom det vid en videokonferens alltid finns någon som berättar om de personuppgifter som behandlas och förklarar ändamålet med behandlingen, torde det inte behövas några särskilda upplysningar eftersom det framgår av sammanhanget både varför uppgifterna behandlas och om det rör sig om uppgifter om misstänkta eller inte.

Rikspolisstyrelsen undrar också hur bestämmelserna är tänkta att tillämpas när uppgifter behandlas i löpande text. Att ställa upp ett generellt krav på att varje personuppgift i löpande text ska förses med en särskild upplysning är naturligtvis inte rimligt. Som Rikspolisstyrelsen påpekar torde det i de allra flesta fall tydligt framgå av omständigheterna för vilket ändamål uppgifterna behandlas och om uppgifterna avser personer som inte är misstänkta för brott. Om uppgifter behandlas i en särskild textfil bör det liksom för bild- och ljudfiler vara tillräckligt att förse filen med en upplysning och förklarande text om innehållet i filen. Vid övrig behandling i löpande text, t.ex. i särskilda fritextfält i register och andra system, framgår det i regel av sammanhanget varför uppgifterna behandlas. Syftet med bestämmelserna om särskilda upplysningar är framför allt att säkerställa att uppgifter som presenteras utanför sitt sammanhang förses med sådana upplysningar. Återigen är det viktigt att framhålla att frågan om huruvida det behövs särskilda upplysningar således kommer att bli beroende av hur polisen organiserar sina system, framför allt vilka sökmöjligheter som skapas. Om polisen möjliggör s.k. fritextsökningar i ett flertal sammanlänkade system bör det vid sökning på viss uppgift av träffbilden framgå för vilket ändamål den aktuella personuppgiften behandlas. Det bör framgå i vilket ärende eller vilken uppgiftssamling – t.ex. ett särskilt underrättelseprojekt – som uppgiften behandlas. Vidare bör det framgå om personen inte är misstänkt för brott.

Upplysning om ändamålet med behandlingen

Det finns som nyss nämnts både integritetsskyddsskäl och verksamhetsskäl som talar för att det bör framgå för vilket ändamål en uppgift som har gjorts gemensamt tillgänglig behandlas. Från integritetssynpunkt har detta betydelse bl.a. för möjligheterna att genom tekniska förfaranden

eller administrativa bestämmelser kunna styra åtkomsten till vissa uppgifter. En upplysning om ändamålet med behandlingen kan vidare vara en förutsättning för att tillsynsmyndigheterna ska kunna kontrollera att viss behandling är berättigad och sker i enlighet med lagens bestämmelser. Framför allt av verksamhetsskäl är information om ändamålet med behandlingen viktig 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 en tjänsteman ska kunna ta ställning till om uppgiften får och bör behandlas för ett nytt ändamål. En särskild bestämmelse bör därför tas in i den nya lagen med innebörd att det alltid ska framgå för vilket ändamål en personuppgift behandlas. Om en personuppgift behandlas inom ramen för den ovan föreslagna bestämmelsen om övervakning av vissa personer, bör detta framgå särskilt. Detsamma bör gälla om en uppgift behandlas med stöd av bestämmelsen om rapportering till polisens kommunikationscentraler.

En särskild upplysning behövs endast om ändamålet för behandlingen inte framgår på något annat sätt. Som *Rikspolisstyrelsen* påpekar framgår ändamålet normalt av omständigheterna när en uppgift ingår i ett särskilt underrättelseprojekt eller särskilt system med ett visst ändamål.

Upplysning om att personen inte är misstänkt

Det är av stor betydelse för skyddet av den personliga integriteten att polisen behandlar personuppgifter på ett sådant sätt att det framgår om en person behandlas som misstänkt eller om behandlingen sker av någon annan anledning. Därför föreslås att det i lagen ställs krav på att det ska framgå om behandlingen avser uppgifter om en person som inte är misstänkt vare sig för ett konkret brott eller för att ha utövat eller komma att utöva brottslig verksamhet. Detta förhållande bör framgå genom en särskild upplysning eller på något annat sätt. Det kan anmärkas att det redan finns krav på särskilda upplysningar vid behandling av underrättelseuppgifter (14 och 19 §§ polisdatalagen).

Ofta framgår det av omständigheterna att en uppgift avser en person som inte är misstänkt. Någon särskild upplysning behövs då inte. I en förundersökning som gäller misshandel kan det t.ex. framgå att A berörs av förundersökningen endast i egenskap av målsägande. Det kan anmärkas att det i 20 och 21 §§ förundersökningskungörelsen (1947:948) ställs krav på att det ska framgå varför en uppgift om en person antecknas i förundersökningsprotokollet. En särskild fråga är hur man ska förfara med en person som i samma sammanhang är såväl misstänkt som icke misstänkt. Sådana fall är inte ovanliga men i regel bör de inte innebära något problem eftersom det normalt framgår av omständigheterna hur situationen är.

Vidare behöver inte enskilda uppgifter i förhör, inlagor eller i bild- och ljudupptagningar förses med särskilda upplysningar, eftersom det i dessa fall normalt framgår av sammanhanget om en omnämnd – eller på bild synlig – person inte är misstänkt. Det är, som tidigare nämnts, framförallt när uppgifter presenteras utanför sitt sammanhang som det kan behövas särskilda upplysningar.

En viss uppgiftssamling kan också vara sådan till sin natur att det är uppenbart att de personer som ingår i samlingen inte är registrerade som misstänkta. Som exempel kan nämnas en förteckning över målsägande.

Upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak

I Europarådets rekommendation No. R (87) 15 om användningen av personuppgifter inom polissektorn anges att skilda kategorier av lagrade uppgifter så långt som möjligt ska kunna skiljas från varandra efter graden av riktighet och tillförlitlighet (princip 3.2). I synnerhet ska uppgifter som grundar sig på fakta kunna skiljas från uppgifter som har sin grund i omdömen eller personliga värderingar. Det ska således gå att utläsa om den som lämnat uppgifter som sedan registreras kan anses vara tillförlitlig samt graden av riktighet i sak, t.ex. om informationen består av kontrollerade fakta eller endast icke styrkta påståenden. I 16 § andra stycket lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns en bestämmelse om att uppgifter om en person som kan antas ha samband med brottslig verksamhet ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Vid tillkomsten av polisdatalagen övervägdes om en motsvarande bestämmelse borde tas in i den lagen. Den dåvarande regeringen lämnade dock inte något sådant förslag. Regeringen hänvisade till att den föreslagna uppdelningen på belastningsregister, misstankeregister och kriminalunderrättelseregister innebar att bekräftade och konkreta uppgifter kom att skiljas från uppgifter som grundades på skälig misstanke respektive på kriminalunderrättelseverksamhet. Att därutöver i lag ta in bestämmelser om att behandlade uppgifter även skulle förses med upplysning om uppgiftslämnarens trovärdighet ansågs inte befogat (prop. 1997/98:97 s. 104 f.).

I den nya lagen föreslås inte några bestämmelser om personuppgiftsbehandling i kriminalunderrättelseverksamhet eller om kriminalunderrättelseregister. Förslaget är utformat så att det kommer att vara möjligt att i en och samma uppgiftssamling sammanföra uppgifter med skiftande grad av tillförlitlighet. *Rikspolisstyrelsen* uppger att det inom all underrättelseverksamhet finns ett verksamhetsbehov att vid analys av information kunna bedöma källans tillförlitlighet och informationens riktighet i sak. Mot den bakgrunden finns det fog för att i den nya lagen ställa upp ett krav på tilläggsupplysningar motsvarande 16 § andra stycket lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. I den nya lagen bör det alltså tas in en bestämmelse om att uppgifter om personer som kan antas ha samband med brottslig verksamhet ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Bestämmelsen bör inte gälla personuppgiftsbehandling inom ramen för brottsutredning utan enbart underrättelseverksamhet. En förundersökning rör ett konkret brott och det framgår då som regel direkt av sammanhanget varför det har ansetts finnas fog för att behandla uppgifter, t.ex. av förhörsprotokoll eller vittneslistor. Risken för missuppfattningar inom ramen för handläggningen av en sådan utredning är därför liten.

Vidare bör det, som föreslås i promemorian, finnas utrymme för att inte lämna någon tilläggsupplysning i situationer där upplysningen framstår som överflödig. Så kan vara fallet beträffande personuppgifter av helt ”neutral” karaktär, exempelvis uppgifter som har inhämtats från folkbokföringen, vägtrafikregistret och liknande källor.

Rikspolisstyrelsen anser att aktuell tilläggsinformation endast ska behöva lämnas ”så långt detta är möjligt” och hänvisar till att detta uttryckssätt används i princip 3.2. i Europarådets rekommendation. Rikspolisstyrelsen förklarar att man inom polisen använder sig av ett värderingssystem som i stort uppfyller promemorieförslagets krav på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Enligt styrelsen förekommer det emellertid att polisen får del av uppgifter som inte har åsatts en sådan värdering, t.ex. uppgifter från andra än polisiära källor och från utländska brottsbekämpande myndigheter.

De exempel som Rikspolisstyrelsen ger motiverar inte avsteg från den viktiga principen att uppgifterna ska förses med tilläggsinformation. De aktuella uppgifterna bör kunna förses med något slag av notering, t.ex. upplysning om att någon bedömning av källans trovärdighet eller uppgifternas riktighet i sak inte kan göras, eventuellt kompletterad med tillägget att det är en uppgift av utländskt ursprung eller från viss annan källa. En sådan notering – som torde vara av stort värde för dem som får del av en personuppgift – är tillräcklig för att uppfylla kravet på upplysning. I motsats till Rikspolisstyrelsen anser regeringen alltså att det bör krävas mer än att upplysning lämnas så långt detta är möjligt, eftersom en sådan formulering kan uppfattas som en möjlighet att efter en diskretionär bedömning avstå från att lämna upplysningar. Med hänsyn till skyddet för den personliga integriteten bör regleringen vara så tydlig som möjligt. En annan sak är att det i vissa fall saknas förutsättningar att göra bedömningen, men då är som redan framgått en upplysning om detta tillräcklig.

Frågan om bestämmelserna om särskilda upplysningar ska gälla retroaktivt behandlas i avsnitt 18 om ikraftträdande och övergångsbestämmelser.

11 Sökbegränsningar för gemensamt tillgängliga uppgifter

11.1 Allmänt om sökbegränsningar

Regeringens bedömning: För att värna den personliga integriteten bör den nya lagen innehålla bestämmelser som reglerar polisens möjligheter att göra sökningar i gemensamt tillgängliga uppgifter.

Utredningen gör inte någon särskild bedömning i denna del.

Remissinstanserna har inte berört frågan närmare.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians bedömning. *Åklagarmyndighe-*

ten är dock tveksam till att införa begränsningar som inskränker urvalet av de uppgifter som presenteras vid en sökning, eftersom en ofullständig redovisning kan vara mer skadlig än en fullständig. Myndigheten anser att man, mot bakgrund av de övriga instrument som föreslås till skydd för integriteten, helt eller till övervägande del kan avstå från bestämmelser om sökbegränsningar. Enligt myndigheten bör en rimlig utgångspunkt vara att uppgifter som har samlats in för tillåtna syften därefter som huvudregel fullt ut ska få behandlas i enlighet med ändamålen intill dess att uppgifterna ska gallras. *Rikspolisstyrelsen* kritiserar förslaget om sökbegränsningar och anser att bestämmelserna på ett allt för detaljerat sätt reglerar polisens arbetsmetoder. Styrelsen hävdar att det i den föreslagna lagen finns andra bestämmelser än de om sökbegränsningar som bör anses utgöra ett tillräckligt skydd för den personliga integriteten. Styrelsen anför vidare att det IT-stöd som polisen avser att använda är uppbyggt så att varje informationsobjekt ska registreras endast en gång, vilket innebär att polisen måste kunna söka och få fram uppgifter om ett informationsobjekt redan förekommer i systemet. Det innebär enligt styrelsen i sin tur att det för detta syfte måste gå att söka och få fram uppgifter om andra personer än de som räknas upp i förslaget. *Sveriges advokatsamfund* pekar på behovet av att genomlysa hur bestämmelser om sökbegränsningar förhåller sig till reglerna i 2 kap. tryckfrihetsförordningen.

Skälen för regeringens bedömning

Behovet av sökbegränsningar

Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör, som redovisas närmare i avsnitt 6.1, ge polisen möjlighet att utveckla och bygga upp sina system på ett friare sätt. Lagen ska därför vara teknikneutral och endast fastställa ramarna för personuppgiftsbehandlingen. Ett av syftena med den nya lagen är att polisen ska kunna dra nytta av insamlad information på ett bättre sätt. Den nya lagstiftningen kommer således att medge ett ökat informationsflöde inom polisen. *Rikspolisstyrelsen* och *Åklagarmyndigheten* invänder mot de föreslagna reglerna om sökbegränsningar och anser att de i alltför stor utsträckning begränsar tillgången till relevanta uppgifter. Sett från integritetssynpunkt är en av de viktigaste aspekterna med behandling av personuppgifter i vilken utsträckning uppgifter kan sökas och sammanställas. Ju större möjligheter det finns att på olika sätt sammanställa uppgifter om enskilda, desto större blir riskerna för intrång i enskildas integritet. I lagstiftning som rör personuppgiftsbehandling finns därför i regel olika bestämmelser som begränsar möjligheten att söka och sammanställa information, t.ex. bestämmelser om vilka sökbegrepp som får användas eller andra typer av sökbegränsningar. De möjligheter som den nya lagen ger polisen att behandla personuppgifter och mängden information, skulle – om det inte fanns några sökbegränsningar – skapa utrymme för kvalificerade former av kartläggning av enskildas personliga förhållanden, vilket i sig kan utgöra ett intrång i den personliga integriteten. Mot denna bakgrund bör det i lagen finnas bestämmelser om sökbegränsningar när det gäller sådana uppgifter som är gemensamt

tillgängliga, dvs. som fler än ett fåtal tjänstemän har tillgång till. Från dessa bestämmelser föreslås dock vissa generella undantag.

Rikspolisstyrelsen anser att de föreslagna sökbegränsningarna innebär en alltför detaljerad styrning av polisens sätt att arbeta. Enligt regeringens mening bör begränsningar av detta slag vara tydliga och konkreta för att ge nödvändig vägledning, samtidigt som de inte i onödan hindrar utvecklingen av nya metoder för polisarbetet eller begränsar möjligheterna att hantera nya former av kriminalitet. Det kan antas att de föreslagna begränsningarna på något sätt kommer att integreras i polisens IT-system, på samma sätt som exempelvis behörigheten för tjänstemännen. Om så blir fallet kommer den enskilde tjänstemannen inte att behöva ta ställning till om begränsningarna är tillämpliga eller inte.

Rikspolisstyrelsen pekar på att sökbegränsningar kan skapa problem vid den tekniska uppbyggnaden av polisens IT-stöd, eftersom detta är tänkt att fungera så att varje informationsobjekt ska registreras endast en gång. Det förutsätter att det går att få fram uppgifter om att ett informationsobjekt redan finns inlagt i systemet. När det gäller frågan om den tekniska uppbyggnaden av polisens IT-stöd bör det enligt regeringens bedömning göras skillnad mellan att registrera nya uppgifter i systemet och att söka efter information. De sökbegränsningar som föreslås torde inte utgöra hinder mot att det i polisens IT-stöd finns en teknisk funktion som hindrar att samma uppgift registreras flera gånger.

Utgångspunkter vid utformningen av sökbegränsningar

Eftersom den nya lagen ger utrymme för att samla in och lagra en mängd olika personuppgifter i samma system kan det finnas uppgifter om samma individ i flera olika sammanhang. Det kan röra sig om allt ifrån ren underrättelseinformation till uppgifter om att personen i fråga har gjort en stöldanmälan eller förekommer som vittne i en förundersökning. En utgångspunkt vid utformningen av sökbegränsningar bör vara att inte alla tjänstemän inom polisen vid varje form av sökning ska kunna göra en sammanställning av all den information som finns i polisens system om en viss person. Polisens allmänna informationsbehov motiverar inte att polisen ges så stora möjligheter att sammanställa och få tillgång till uppgifter. Såväl sekretessregleringen som integritetsintressen talar också mot en sådan lösning. Dessutom står det inte i rimlig proportion till det integritetsintrång som det skulle kunna innebära för den enskilde att låta den som t.ex. gör en rutinmässig sökning när någon har ertappats för fortkörning få tillgång till all information om den kontrollerade. Däremot finns det situationer där vissa tjänstemän inom polisen måste kunna göra mer omfattande sökningar. Den nya lagen måste ge utrymme för en sådan flexibilitet. Vidare bör lagen medge att en polisman som har fått fram en grunduppgift, t.ex. om att den sökta personen är misstänkt för brott, söker efter ytterligare information, i den utsträckning det finns skäl för det.

I lagen bör även införas bestämmelser som begränsar användningen av känsliga personuppgifter som sökbegrepp. I avsnitten 11.2 och 11.3 redogörs närmare för hur sökbegränsningarna bör utformas.

Sveriges advokatsamfund efterfrågar en analys av hur förslagen om sökbegränsningar förhåller sig till reglerna i 2 kap. tryckfrihetsförordningen. Varje sammanställning av personuppgifter som en myndighet kan göra med hjälp av tillgänglig teknik och rutinbetonade åtgärder är i princip att anse som en allmän handling hos myndigheten, oavsett om sammanställningen behövs för myndighetens egen verksamhet eller inte. Sådana sammanställningar utgör s.k. potentiella handlingar. Elektroniskt lagrade handlingar som har ett fixerat innehåll som går att återskapa gång på gång, t.ex. e-brev eller protokoll i elektronisk form, utgör s.k. färdiga elektroniska handlingar. Om den myndighet som förvarar elektroniskt lagrade personuppgifter är förbjuden att göra sammanställningar med hjälp av vissa sökbegrepp har inte allmänheten rätt att begära ut en sådan sammanställning. Detta framgår av 2 kap. 3 § tredje stycket tryckfrihetsförordningen (begränsningsregeln). Bestämmelsen är inte tillämplig på s.k. färdiga elektroniska handlingar (prop. 2001/02:70 s. 38).

Bestämmelser om förbud mot att använda vissa sökbegrepp är alltså av betydelse även för bedömningen av vilka handlingar som utgör allmänna handlingar hos en myndighet. Bestämmelser om för vilka ändamål personuppgifter får behandlas i en myndighets verksamhet, s.k. ändamålsbegränsningar, inskränker dock inte en myndigheters skyldighet enligt offentlighetsprincipen att sammanställa personuppgifter (se bl.a. SOU 2004:6 s. 246 och prop. 2007/08:160 s. 69 f.). I det följande föreslås ett förbud mot att använda känsliga personuppgifter som sökbegrepp. Ett sådant förbud får genomslag vid tillämpningen av 2 kap. tryckfrihetsförordningen. Däremot får förslaget om begränsningar vid sökning på personnummer och liknande identitetsuppgifter inte den effekten.

Bestämmelserna i tryckfrihetsförordningen kompletteras av offentlighets- och sekretesslagen (2009:400), som innehåller bestämmelser om bl.a. sekretess i polisens verksamhet. Sådana bestämmelser finns bl.a. i lagens 35 kap., som innehåller bestämmelser till skydd för enskildas integritet.

11.2 Känsliga personuppgifter som sökbegrepp

Regeringens förslag: Känsliga personuppgifter ska inte få användas som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Det ska dock inte finnas något hinder mot att använda brottsrubriceringar eller uppgifter som beskriver en persons utseende som sökbegrepp.

Utredningen lämnar inte några förslag i denna del.

Remissinstanserna har inte berört frågan närmare.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian förtydligas inte att det är tillåtet att använda brottsrubriceringar som sökbegrepp.

Remissinstanserna: Det stora flertalet av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Rikspolisstyrelsen* anför att det är viktigt att polisen i vissa fall kan använda känsliga personuppgifter som sökbegrepp för att kartlägga vissa typer av brottslig

verksamhet, t.ex. hatbrott och sexualbrott. Styrelsen anser därför att frågan om känsliga personuppgifter som sökbegrepp bör analyseras närmare.

Skälen för regeringens förslag: Vissa slag av uppgifter är till sin natur särskilt integritetskänsliga, i synnerhet uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och uppgifter som rör hälsa eller sexualliv. Detta kommer till uttryck bl.a. genom bestämmelser i dataskyddsdirektivet och i dataskyddsrambeslutet (se avsnitt 4.2.5 och 4.4.1) om särskilda begränsningar i rätten att behandla känsliga personuppgifter. I avsnitt 8 föreslås därför att känsliga personuppgifter som huvudregel inte ska få behandlas, men att uppgifter om en person som behandlas på annan grund ska få kompletteras med känsliga personuppgifter när det är absolut nödvändigt för syftet med behandlingen. Det innebär att det i polisens olika uppgiftssamlingar kommer att finnas känsliga personuppgifter.

Sökning på känsliga personuppgifter inger särskilda betänkligheter. Sådana sökningar skulle kunna möjliggöra exempelvis kartläggning av personer med viss politisk ståndpunkt eller religiös inriktning. Mot den bakgrunden har det i 20 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet föreskrivits förbud mot att använda känsliga personuppgifter som sökbegrepp. Bestämmelser med motsvarande förbud finns även i förslagen till lag om behandling av uppgifter i Kustbevakningens verksamhet i betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18) och lag om behandling av uppgifter i åklagarväsendets brottsbekämpande verksamhet i betänkandet Åklagarväsendets brottsbekämpning Integritet – Effektivitet (SOU 2008:87). *Rikspolisstyrelsen* framhåller att det är viktigt för polisen att i vissa situationer kunna använda sig av känsliga personuppgifter som sökbegrepp. Det kan, enligt regeringens mening, i och för sig finnas situationer då en sådan möjlighet skulle vara av värde för det brottsbekämpande arbetet, t.ex. vid utredningen av ett sexualbrott eller ett våldsbrott med stark koppling till politisk eller religiös fanatism samt vid kartläggning av hatbrott. Normalt bör dock andra möjligheter till sökningar i t.ex. belastnings- och misstankeregistren eller i andra uppgiftssamlingar hos polisen utgöra ett tillräckligt stöd i det brottsbekämpande arbetet. Vidare bör framhållas att bestämmelsen inte hindrar sökning på brottsrubriceringar, t.ex. våldtäkt eller sexuellt övergrepp mot barn. Detta bör tydliggöras i lagtexten.

Sammantaget väger enligt regeringens mening integritetsintresset över. I den nya lagen bör det därför finnas en bestämmelse som föreskriver att känsliga personuppgifter inte får användas som sökbegrepp i polisens brottsbekämpande arbete.

Signalementsuppgifter har stor betydelse i brottsbekämpningen. Vid exempelvis sökandet efter misstänkta gärningsmän behöver polisen kunna använda sig av uppgifter om t.ex. kroppsbyggnad, ansiktsform, hår- eller hudfärg, klädsel och fysiska kännetecken som födelsemärken, tatueringar och synbara fysiska defekter. Förbudet mot att använda känsliga personuppgifter som sökbegrepp bör därför inte hindra att uppgifter som beskriver en persons utseende används som sökbegrepp. Detta – som överensstämmer med vad som gäller enligt lagen om behandling av

uppgifter i Tullverkets brottsbekämpande verksamhet – bör komma till uttryck i den nya lagen.

11.3 Sökning på namn, personnummer eller samordningsnummer

Regeringens förslag: Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga, får sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva viss brottslig verksamhet,
4. övervakas på grund av allvarlig kriminell belastning eller för att personen kan antas utgöra ett hot mot andras personliga säkerhet,
5. har anmält ett brott,
6. är målsägande i ett ärende som rör ansvar för brott,
7. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,
8. har gett in eller tillhandahållits en handling,
9. är anmäld såsom försvunnen,
10. har bedömts kunna komma att möta ett polisingripande med grovt våld, eller
11. är efterlyst.

De nu angivna begränsningarna ska dock inte gälla vid sökning i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Begränsningarna ska inte heller gälla vid sökning som utförs av särskilt angivna tjänstemän och som görs

a) för att förebygga, förhindra eller upptäcka särskilt allvarlig brottslig verksamhet,

b) för övervakning av personer som kan antas komma att begå brott och som är allvarligt kriminellt belastade eller kan antas utgöra ett hot mot andras personliga säkerhet, eller

c) för att utreda särskilt allvarliga brott.

Regeringen har möjlighet att meddela föreskrifter om ytterligare undantag från bestämmelserna om sökbegränsningar.

Utredningen lämnar inte något förslag i denna fråga.

Remissinstanserna har inte berört frågan närmare.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian innehåller dock inte något förslag om att uppgifter om personer som har bedömts kunna komma att möta ett polisingripande med grovt våld eller personer som är efterlysta får tas fram vid sökning i gemensamt tillgängliga uppgifter. Den innehåller heller inte någon bestämmelse om att regeringen eller den myndighet som regeringen be-

stämmer kan meddela föreskrifter om begränsning av tillgången till vissa kategorier av uppgifter eller någon bestämmelse som ger möjlighet för regeringen att meddela föreskrifter om ytterligare undantag från bestämmelserna om sökbegränsningar. I promemorian föreslås att sökbegränsningarna ska gälla även vid sökning på firma och organisationsnummer.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inget att invända mot förslaget. *Åklagarmyndigheten* anför att utformningen av de föreslagna begränsningarna väcker osäkerhet om de helt eller delvis avser endast personuppgifter som är aktuella, alltså uppgifter i öppna, aktiva ärenden. Vidare bör enligt myndigheten klargöras om förslaget ska tolkas så att namn eller personnummer inte ska kunna användas för att identifiera en förundersökning som bör återupptas eller som utgör skäl för att inte inleda en ny förundersökning om samma sak. *Rikspolisstyrelsen* anser att de föreslagna bestämmelserna på ett alltför detaljerat sätt kommer att reglera polisens arbetsmetoder och omöjliggöra det normala arbetssättet vid bekämpning av bl.a. grov organiserad brottslighet. Styrelsen ifrågasätter också om förslaget, vars grundmotiv är att skydda den personliga integriteten, verkligen bör gälla juridiska personer. Enligt styrelsen kommer även det internationella polisiära samarbetet, bl.a. när det gäller Europols informationssystem EIS, att avsevärt försvåras av de föreslagna begränsningarna avseende juridiska personer. Det finns enligt Rikspolisstyrelsen ett stort behov av att kunna söka på personnummer eller liknande identitetsbeteckningar och få besked om personen förekommer i polisens uppgiftssamlingar eller inte. Styrelsen pekar bl.a. på att det enligt förslaget inte ges någon möjlighet att flagga upp för den som söker information att den person som är föremål för sökningen är av intresse i t.ex. ett underrättelseprojekt. För att arbetet på kommunikationscentralerna ska fungera är det enligt Rikspolisstyrelsen viktigt att det på ett enkelt och effektivt sätt går att få fram uppgifter om att en person är farlig eller är efterlyst samt anledningen till efterlysningen. Styrelsen anser därför att förslaget bör kompletteras med bestämmelser som möjliggör att sådan information tas fram. I syfte att göra författningstexten mer enhetlig föreslår Rikspolisstyrelsen vidare att formuleringen av den föreslagna bestämmelsen om särskilt angivna tjänstemän med vissa uppgifter anpassas till den formulering som föreslagits när det gäller tillgången till personuppgifter.

Kustbevakningen anser att ett annat begrepp än ordet misstänkt bör användas i relation till uppgifter som rör en person som har någon form av samband med misstänkt brottslig verksamhet. *Skatteverket* instämmer i promemorians bedömning att det behövs begränsningar som hindrar att alla uppgifter om en fysisk person kan sökas fram i alla lägen. Uppgifter om juridiska personer och fysiska personer knutna till en juridisk person bör däremot enligt verket få tas fram. Enligt Skatteverkets uppfattning bör det dessutom alltid vara möjligt att bekräfta om en uppgift förekommer eller inte bland de personuppgifter som får göras gemensamt tillgängliga. *Datainspektionen* anser att förslaget inte är tillräckligt genomarbetat då det bl.a. saknas en analys av de effekter som utformningen av sökbegränsningarna kan väntas ge. Datainspektionen anför bl.a. att begränsningarna enbart gäller den initiala sökningen och endast vissa typer av sökningar. De relativt omfattande undantagen från sökbegränsningarna kommer enligt inspektionen sannolikt att medföra att avancerade

sökmöjligheter – utan de föreslagna sökbegränsningarna – kommer att byggas in i polisens system. Enligt Datainspektionen kommer de föreslagna begränsningarna med stor sannolikhet att sakna större betydelse för integritetsskyddet.

Skälen för regeringens förslag

Får sökning göras på personnummer och liknande uppgifter?

Som framgår av avsnitt 11.1 är utgångspunkten att polisen inte vid varje tillfälle och i varje situation ska kunna göra en sökning som kan leda till en kartläggning av om en viss person förekommer i den polisiära verksamheten. Frågan är då hur polisens informationsinhämtning ska begränsas.

Det är självklart att polisen gör sökningar med hjälp av bl.a. personnummer. Namn och personnummer är viktiga för identifieringen av en person och kontrolleras regelmässigt i samband med brottsutredningar och annat brottsbekämpande arbete. Detsamma gäller samordningsnummer, dvs. sådana identitetsbeteckningar som enligt 18 a § folkbokföringslagen (1991:481) kan tilldelas personer som inte är eller har varit folkbokförda i Sverige. Personuppgifter av nu aktuellt slag måste i stor utsträckning användas i brottsutredningar för att undanröja risken för personförväxling. Det är uppenbart att möjligheten att göra sökningar på sådana uppgifter även kan vara av betydelse vid underrättelseverksamhet. Det bör t.ex. vara möjligt att inom ramen för det arbete som bedrivs i en undersökning som avser viss misstänkt brottslig verksamhet, söka fram uppgifter om huruvida personer som figurerar i det ärendet också är misstänkta i andra ärenden. Den nya lagen bör således ge utrymme för sökningar på namn, personnummer och andra liknande identitetsbeteckningar.

Användandet av detta slag av uppgifter som sökbegrepp kan emellertid ge upphov till särskilda risker från integritetssynpunkt. En sökning på exempelvis ett personnummer kan, i vart fall om den sker i den samlade informationsmängd som polisen har tillgång till, ge möjlighet till kartläggning av en persons privata förhållanden. Från ett integritetsperspektiv är sådana sökningar ägnade att inge betänkligheter. Mot den bakgrunden bör en obegränsad möjlighet att göra sökningar med hjälp av detta slag av uppgifter inte införas.

I promemorian övervägs om det i den nya lagen bör tas in en bestämmelse motsvarande 21 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Enligt den bestämmelsen får namn, personnummer och samordningsnummer användas som sökbegrepp bara om uppgifterna avser en person som är misstänkt för något visst brott eller för viss brottslig verksamhet. I promemorian görs dock bedömningen att en sådan bestämmelse inte är ändamålsenlig på polisens område. Regeringen delar den bedömningen, särskilt mot bakgrund av att en sådan bestämmelse inte tillåter att det görs vissa sökningar som kan vara nödvändiga inom ramen för ett underrättelseprojekt. I ett sådant ärende kan det vara av vikt att kunna klarlägga om personer som har anknytning till den undersökta verksamheten – men som vid den tidpunkten inte är misstänkta – förekommer som misstänkta i andra underrättelseprojekt eller i

brottsutredningar som gäller liknande brott. I brottsutredningar rörande allvarliga brott, där det inte finns någon misstänkt person, måste polisen också ha möjlighet att göra mer omfattande sökningar. Uppgifter om andra personer än misstänkta kan också – satta i ett större sammanhang – vara viktiga pusselbitar vid utredningen av ett brott eller i ett underrättelseprojekt. Mot bakgrund härav bör möjligheten att söka på namn, personnummer och liknande identitetsuppgifter också omfatta andra än misstänkta personer i vissa fall.

I promemorian föreslås att möjligheten att söka på identitetsbeteckningar som avser juridiska personer ska begränsas på samma sätt som när det gäller fysiska personer. Detta ifrågasätts av *Rikspolisstyrelsen* och *Skatteverket*, som anför att det inte finns samma behov av integritetsskydd för juridiska personer som för fysiska personer.

Uppgifter om juridiska personer behandlas ofta i polisens verksamhet bl.a. på grund av att t.ex. aktiebolag inte sällan används som brottshjälpmedel. Vid utredning och kartläggning av exempelvis organiserad ekonomisk brottslighet är sökning på firma eller organisationsnummer för att hitta samband och kopplingar mellan olika personer en viktig del i det polisiära arbetet. Det finns således ett tydligt polisiärt behov av att kunna söka på uppgifter om juridiska personer. Behovet av integritetsskydd, exempelvis skydd mot kartläggning är inte heller lika stort för juridiska personer som för fysiska personer. Till detta kommer att uppgifter om juridiska personer i stor utsträckning redan förekommer i offentliga register, bl.a. hos Bolagsverket. Som *Rikspolisstyrelsen* påpekar kan promemorians förslag i denna del också skapa svårigheter i det internationella samarbetet. Det bör därför inte införas några bestämmelser som begränsar möjligheten att göra sökningar beträffande juridiska personer.

När det gäller frågan hur möjligheten att göra sökningar närmare bör regleras delar regeringen promemorians bedömning att det i lagen uttryckligen bör anges vilka uppgifter som får tas fram vid en sökning på identitetsbeteckningar som avser en fysisk person. Den frågan behandlas i det följande.

Vilka sökningar bör omfattas av sökbegränsningar?

Polisen har olika behov av att kunna få fram uppgifter om personer beroende på i vilket sammanhang frågan aktualiseras. En första fråga är därför om de begränsningar som ska gälla för sökning på personnummer och liknande identitetsbeteckningar ska gälla i alla situationer där polisen gör en sökning med hjälp av personnummer eller endast i vissa situationer. Man kan, mycket förenklat, peka ut vissa typsituationer där polisen söker information med utgångspunkt i personuppgifter. Det kan röra sig om situationer där det utförs en allmän polisiär kontroll av något slag, t.ex. en trafikkontroll, kontroll av ungdomar som befinner sig i utsatta situationer eller kontroll i samband med ordningsproblem. I de fallen kan det vara fråga om en ren identitetskontroll eller kontroll av behörighet att föra fordon eller liknande. Det kan vidare vara fråga om att någon person begär upplysningar eller att få ta del av handlingar i den brottsbekämpande verksamheten eller att polis eller åklagare söker efter ett tidigare

ärende. I de fallen utgör personnumret ofta nyckeln till att hitta rätt ärende. Det kan även röra sig om kommunikationscentralens behov av att ta fram personuppgifter i samband med larm om brott eller ordningsstörningar. Därutöver kan det vara fråga om kontroller som görs på personer inom ramen för en brottsutredning (vittnen, misstänkta och andra personer). Det kan även röra sig om underrättelseverksamhet, där kartläggning av miljöer, företeelser och personer utgör en viktig beståndsdel. Polisen behöver alltså kunna använda sig av personnummer och liknande identitetsbeteckningar som sökbegrepp i många olika sammanhang och det går inte att enbart utifrån de olika verksamhetsbehoven avgöra vilka sökningar som ska omfattas av särskilda sökbegränsningar. Den frågan måste avgöras även utifrån andra kriterier.

Vid avgörandet av vilka sökningar som bör omfattas av sökbegränsningar kan inledningsvis konstateras att de integritetsrisker som motiverar inskränkningarna inte gör sig gällande i samma utsträckning när det är fråga om sökningar i ett *begränsat material*, exempelvis en viss handling eller ett visst ärende. Det är från effektivitetssynpunkt dessutom rimligt att en tjänsteman som arbetar i ett elektroniskt dokument får söka fritt i det dokumentet genom att t.ex. använda sedvanliga sökfunktioner i ett ordbehandlingsprogram. Det finns därför inte skäl att införa sökbegränsningar vid sökning i en viss handling eller ett visst ärende. I sådant arbete som bedrivs inom ramen för en särskild undersökning enligt 14 § polisdatalagen och som avser viss brottslighet (t.ex. narkotikabrottslighet i en viss region) eller vissa kriminella grupperingar (t.ex. ett mc-gäng) upprättas ofta särskilda uppgiftssamlingar. Dessa uppgiftssamlingar syftar till att kartlägga en viss brottslighet eller en viss kriminell gruppering och endast de tjänstemän som deltar i undersökningen har tillgång till dem. Även i dessa fall är det fråga om ett begränsat material som, trots att det i regel är fråga om gemensamt tillgängliga uppgifter, endast en begränsad krets av personer har tillgång till. Mot denna bakgrund bör det som promemorian föreslår även vara möjligt att fritt göra sökningar i en sådan uppgiftssamling.

För vissa delar av den brottsbekämpande verksamheten kan begränsningar i sökmöjligheterna leda till särskilda problem som motiverar att den personliga integriteten i viss mån får stå tillbaka för kravet på en effektiv brottsbekämpning. Det gäller bl.a. *underrättelseverksamhet som avser särskilt allvarlig brottslighet* som t.ex. grova narkotikabrott, terroristbrott och människohandel. Här finns det ett påtagligt polisiärt behov av att kunna göra mer omfattande sökningar. Det bör därför inte införas några sökbegränsningar vid sökning som görs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver. En förutsättning för detta bör dock vara att sökningen utförs av tjänstemän som har tilldelats särskild behörighet att utföra sådana sökningar. Dessa tjänstemän bör få utföra mer omfattande sökningar, exempelvis i flera olika uppgiftssamlingar om viss brottslighet eller vissa kriminella grupperingar. Vilka kategorier av tjänstemän som bör tilldelas denna särskilda behörighet och hur många tjänstemän det kan bli fråga om beror på hur polisen organiserar sin verksamhet. Det bör kunna vara fråga om allt ifrån ett fåtal utpekade personer vid en myndighet till samtliga personer på en rotel som har till uppgift att hantera t.ex. underrättelseverksamhet som avser särskilt

allvarlig brottslighet. Det bör meddelas föreskrifter om vilka närmare kvalifikationskrav m.m. som bör ställas på dessa tjänstemän och på att myndigheten dokumenterar vilka tjänstemän som har beviljats denna utökade möjlighet att söka efter uppgifter. Det är således inte, som *Rikspolisstyrelsen* förordar, tillräckligt att luta sig mot den föreslagna bestämmelsen som föreskriver att en tjänsteman vid fullgörandet av sina arbetsuppgifter endast får ha åtkomst till de uppgifter han eller hon behöver för att fullgöra dessa.

Vid *övervakning av vissa personer,* som kan antas komma att begå brott och som är allvarligt kriminellt belastade eller kan antas utgöra ett hot mot andras personliga säkerhet, finns ett likartat behov av att kunna göra mera omfattande sökningar. I sådana fall är det viktigt för polisen att ha kännedom om var personen brukar befinna sig, vilka kontakter han eller hon har, vilka transportmedel personen förfogar över etc., för att polisen ska kunna ingripa i tid mot nya brott. Sökbegränsningar bör därför inte gälla för sökningar som utförs som ett led i sådan övervakning. På samma sätt som när det gäller sökning i viss underrättelseverksamhet bör det dock även i dessa fall krävas att sökningen utförs av särskilt angivna tjänstemän.

Ibland kan det också finnas behov av att göra mera omfattande sökningar inom ramen för en *förundersökning om ett allvarligt brott*. Som exempel kan nämnas utredningar om ouppklarade allvarliga seriebrott, t.ex. upprepade våldtäkter eller mordbränder. Detsamma kan gälla vissa mordutredningar. Förundersökningar om sådana brott kan pågå under mycket lång tid, om gärningsmannen är okänd. Om det är fråga om mycket allvarliga brott, där samhällets intresse av att gärningsmannen lagförs är stort, är det försvarligt att tillåta mera omfattande sökningar om dessa kan bidra till att polisen kan spåra gärningsmannen. En lämplig avvägning är att det ska vara fråga om brott för vilket är föreskrivet fängelse i fyra år eller däröver. I likhet med vad som föreslagits i fråga om sökningar i underrättelseverksamhet eller vid övervakning av vissa personer bör emellertid sådana sökningar enbart få utföras av på förhand utpekade personer med särskilda arbetsuppgifter.

För andra situationer än de nu nämnda, dvs. vid annan sökning än i begränsade uppgiftsmängder, i underrättelseverksamhet som rör särskilt allvarlig brottslig verksamhet, vid övervakning av vissa personer och i förundersökningar om allvarliga brott, bör lagen innehålla bestämmelser som begränsar träffbilden vid sökningar på personnummer eller liknande identitetsbeteckningar.

Det kan dock inte uteslutas att det finns andra situationer än de nu nämnda där polisen har särskilda behov av att kunna söka och sammanställa information, t.ex. för att upprätthålla vissa specifika funktioner inom klart avgränsade områden. Ett exempel skulle kunna vara sådana tjänstemän med beredningsfunktioner inom underrättelseverksamhet som Rikspolisstyrelsen omnämner i redovisningen av det uppdrag som beskrivs närmare i avsnitt 3. Mot denna bakgrund bör regeringen ha möjlighet att meddela föreskrifter om ytterligare undantag från de föreslagna sökbegränsningarna.

Vilka uppgifter bör få tas fram vid en sökning?

En regel om sökbegränsningar måste självfallet utformas så att uppgifter som det generellt sett finns ett stort behov av får tas fram. Frågan är då vilka uppgifter som är sådana att de bör ingå i träffbilden vid en sökning som omfattas av sökbegränsningar.

Först och främst bör det vara möjligt att ta fram uppgifter som anger att den sökte har anmälts för brott eller är misstänkt för brott eller för allvarlig brottslig verksamhet eller brottslighet som sker systematiskt. Med allvarlig brottslig verksamhet avses här detsamma som i avsnitt 9.2, dvs. verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver. Även uppgifter om att den sökte tidigare har varit misstänkt för brott bör kunna tas fram. Detta överensstämmer i huvudsak med vad som föreslås i promemorian. För att undanröja den oklarhet som *Åklagarmyndigheten* påtalar bör dock tydliggöras att även personuppgifter i avslutade ärenden får tas fram, så länge övriga krav för att få behandla sådana uppgifter är uppfyllda. Att även uppgifter om tidigare misstankar ska kunna tas fram motiveras bl.a. av att sådana kan behövas för att identifiera t.ex. en förundersökning som lagts ned och som bör återupptas. Det förtjänar att påpekas att detta inte innebär att en person som tidigare har varit misstänkt får pekas ut som misstänkt i polisens system. Är det fråga om en avslutad förundersökning där någon tidigare har varit misstänkt måste det tydligt framgå att personen i fråga inte längre är misstänkt (jfr avsnitt 10 och 14.4.).

Kustbevakningen anser att ett annat begrepp än misstänkt bör användas i relation till uppgifter som rör en person som har samband med misstänkt brottslig verksamhet. När polisen behandlar personuppgifter i underrättelseverksamhet är det viktigt, både av verksamhets- och integritetsskäl, att det klart framgår varför uppgifterna behandlas och om personen i fråga är eller har varit misstänkt för brottslig verksamhet eller om denne endast har andra kopplingar till sådan verksamhet, och alltså inte själv är eller har varit misstänkt. Det behövs därför ett begrepp som klart uttrycker denna skillnad. Begreppet ”misstänkt” används i samband med brottslig verksamhet i bl.a. 19 § polisdatalagen och 21 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Mot bakgrund härav finner regeringen inte skäl att använda något annat begrepp.

I likhet med vad som föreslås i promemorian bör det även vara möjligt att få fram uppgift om huruvida en person övervakas på grund av allvarlig kriminell belastning eller befarad farlighet för annans personliga säkerhet.

En annan uppgift som bör vara möjlig att få fram är att personen har anmält ett brott eller att han eller hon förekommer som målsägande eller vittne i en brottsutredning. Detsamma bör gälla om någon är anmäld såsom försvunnen. Det bör också vara möjligt att få fram uppgift om en handling har lämnats in av eller expedierats till personen i fråga.

Rikspolisstyrelsen anser att det för att arbetet på kommunikationscentralerna ska fungera bör vara möjligt att få fram uppgifter om att en person är farlig eller efterlyst.

Polisens kommunikationscentraler har till uppgift att ta emot och vidarebefordra inkommande larm och andra meddelanden samt att inled-

ningsvis vidta och samordna polisåtgärder med anledning av den inkommande informationen. Det är ofta fråga om brådskande situationer som kräver omedelbara åtgärder. För att uppgifterna ska kunna utföras på ett tillfredsställande sätt är det viktigt att personalen på kommunikationscentralerna snabbt kan få fram nödvändig och relevant information. En del av de situationer där polisen tvingas att ingripa kan medföra risker både för allmänheten och för den enskilde polismannen. Så kan t.ex. vara fallet vid ingripanden mot en person som innehar ett vapen och som kan misstänkas komma att bruka detta vid ingripandet. Det kan även vara fråga om ingripanden mot personer som av andra skäl bedöms kunna komma att utgöra en allvarlig fara för sig själv, för allmänheten eller för polispersonalen i samband med ingripandet. Uppgifter om att en person har bedömts kunna komma att möta ett ingripande med grovt våld kan i dessa situationer vara avgörande för planeringen och samordningen av polisiära åtgärder. Sådan information bör därför få tas fram vid en sökning. Det bör dock framhållas att det krävs noggranna överväganden innan den nu aktuella bedömningen kan göras och att en notering om en sådan bedömning kan ifrågasättas ur ett integritetsperspektiv. Detta bör därför förekomma endast under förutsättning att det finns konkreta omständigheter som talar för en sådan bedömning. Det kan t.ex. vara fråga om att personen vid tidigare ingripanden varit beväpnad eller våldsam. Rikspolisstyrelsen bör kunna utfärda riktlinjer för under vilka förutsättningar en person kan bedömas kunna komma att möta ett polisingripande med grovt våld och när och hur en notering om en sådan bedömning bör ske.

Även uppgiften att en person är efterlyst är viktig information i det polisiära arbetet. Sådana uppgifter bör också få tas fram vid en sökning.

Några av de kategorier av personuppgifter som nu har nämnts är till sin natur av mera känsligt slag. Det gäller särskilt uppgifter om att en person tidigare har varit misstänkt för brott, uppgifter om att en person är misstänkt för brottslig verksamhet och uppgifter om att en person övervakas. Behovet av att få tillgång till sådana uppgifter skiljer sig dessutom åt beroende på i vilket sammanhang sökningen sker. I många fall torde behovet av sådan information vara begränsat. Något behov av att t.ex. få tillgång till uppgifter om tidigare brottsmisstankar vid en rutinsökning i samband med en trafikkontroll finns knappast. Det torde i regel inte heller finnas behov av att få tillgång till underrättelseinformation vid en sådan sökning. Generellt sett torde behovet av information om samtliga sökbara kategorier av personuppgifter vara störst i underrättelseverksamhet och i samband med utredning av vissa typer av brott. Av integritetshänsyn bör tillgången till dessa kategorier av uppgifter begränsas. Föreskrifter om sådana begränsningar bör lämpligen meddelas av regeringen eller den myndighet som regeringen bestämmer.

Rikspolisstyrelsen lyfter fram behovet av att alltid kunna få besked om en viss person förekommer eller inte i polisens system och att kunna markera för den som söker information att den person som är föremål för sökningen är av intresse i t.ex. ett visst underrättelseprojekt. Även *Skatteverket* anser att det alltid bör vara möjligt att få besked om en person förekommer eller inte i polisens system. I vissa situationer kan det visserligen finnas ett behov av att kunna få träff på personer som inte omfattas av någon av de personkategorier som föreslås i promemorian eller

att kunna markera att den sökta personen är av intresse i t.ex. viss underrättelseverksamhet. Det behovet måste dock vägas mot integritetsskyddsintressen. Den nya lagen kommer att ge polisen utökade möjligheter att behandla personuppgifter i bl.a. underrättelseverksamhet. För att detta ska vara godtagbart ur ett integritetsperspektiv bör lagen innehålla bestämmelser som motverkar otillbörlig övervakning eller kartläggning av enskildas personliga förhållanden. Att endast vissa uppgifter är sökbara vid flertalet allmänna sökningar utgör en sådan begränsning. En sådan ”hit/no-hit funktion” som Rikspolisstyrelsen och Skatteverket efterfrågar bör inte möjliggöras i den nya lagen. Som anförs i avsnitt 11.1 hindrar detta emellertid inte att det i polisens system finns tekniska funktioner som hindrar att samma uppgift registreras flera gånger.

Det förtjänar att framhållas att de begränsningar som nu föreslås endast omfattar den initiala sökningen. En allmän sökning som görs med hjälp av personnummer eller motsvarande identitetsbeteckning ska alltså, enligt förslaget, ge en första träffbild som innefattar endast någon eller några av de kategorier som anges i förslaget. Sedan man väl har fått träff på en viss person, exempelvis som misstänkt för brott i en viss förundersökning, ska ytterligare uppgifter kunna tas fram genom en fortsatt behandling i den uppgiftsmängden. Möjligheten att få tillgång till ytterligare uppgifter, kanske hela förundersökningen, avgörs av vilken behörighet den berörda tjänstemannen har och om behandlingen behövs för något av lagens ändamål.

Konsekvenser av de föreslagna sökbegränsningarna

Rikspolisstyrelsen riktar kritik mot förslaget om sökbegränsningar, och anser bl.a. att bestämmelserna på ett allt för detaljerat sätt reglerar polisens arbetsmetoder. Som framgått ovan tillgodoses styrelsens synpunkter i vissa delar. De sökbegränsningar som föreslås vid en initial allmän sökning torde inte vara av sådan karaktär att de påtagligt inskränker polisens frihet att välja arbetsmetoder.

Datainspektionen efterfrågar en analys av de effekter som utformningen av sökbegränsningarna kan väntas ge. Inspektionen anför att sökbegränsningarna med stor sannolikhet kan komma att sakna större betydelse för integritetsskyddet. Inspektionens slutsats synes grunda sig både på hur reglerna om sökbegränsningar har utformats och utformningen av lagen i stort. Det ligger i sakens natur att inskränkningar i möjligheten att göra sökningar begränsar spridningen av uppgifter. Detta gäller även om inskränkningarna bara omfattar den initiala sökningen och det finns andra undantag. I många fall torde någon sökning utöver den initiala inte bli aktuell, exempelvis därför att personen som eftersöks inte tillhör någon av kategorier som ger träff vid sökning på personnummer. I andra fall är de uppgifter som kommer fram om personen ointressanta och i åter andra fall kan ytterligare sökning hindras om polismannen inte har behörighet att ta del av uppgifterna. Att det kan vara svårt att i alla avseenden överblicka konsekvenserna av begränsningarna innebär således inte att dessa kan frånkännas betydelse. De sökbegränsningar som föreslås är enligt regeringens bedömning väl avvägda och utgör ett skydd för den personliga integriteten.

Det är emellertid viktigt att följa utvecklingen för att, vid behov, kunna göra eventuella förändringar som krävs om det skulle visa sig att de föreslagna sökbegränsningarna inte ger det integritetsskydd som varit avsett. Det är bl.a. mot den bakgrunden viktigt att lagstiftningen utvärderas (se avsnitt 17.3).

12 Informationsutbyte

12.1 Behovet av ett effektivt informationsutbyte mellan brottsbekämpande myndigheter

Regeringens bedömning: En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna kan utbyta information på ett rationellt sätt.

Utredningen behandlar inte frågan särskilt.

Remissinstanserna: Flera remissinstanser, bl.a. dåvarande *Riksåklagaren,* dåvarande *Riksskatteverket, Tullverket* och *Kustbevakningen,* har påtalat behovet av ett effektivt informationsutbyte mellan de brottsbekämpande myndigheterna. De brottsbekämpande myndigheterna har ansett sig ha ett påtagligt behov av att i ökad utsträckning få direktåtkomst till varandras uppgifter.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna instämmer i promemorians bedömning. Flera remissmyndigheter, bland dem *Ekobrottsmyndigheten, Tullverket* och *Kustbevakningen*, understryker behovet av direktåtkomst till vissa uppgifter hos polisen. Några remissinstanser kritiserar den terminologi som används.

Skälen för regeringens bedömning

Informationsutbytet måste kunna effektiviseras

Samarbetet mellan brottsbekämpande myndigheter har blivit allt viktigare i det brottsförebyggande och brottsutredande arbetet. Ett effektivt och framgångsrikt arbete mot allvarlig och organiserad brottslighet förutsätter att man kan dra nytta av den samlade kunskap om brott som finns inte bara inom olika delar av polisorganisationen utan också hos andra brottsbekämpande myndigheter. Informationsutbyte har även betydelse för bekämpning av bl.a. mängdbrottsligheten.

Uppdelningen av den brottsbekämpande verksamheten på olika myndigheter har emellertid i stor utsträckning kommit att styra möjligheterna till informationsutbyte, eftersom sekretess gäller mellan myndigheter. Det är allmänt omvittnat att detta har lett till nackdelar när det gäller effektiviteten i brottsbekämpningen. Av samma skäl som det är viktigt att man inom polisen på ett effektivare sätt kan tillgodogöra sig den information som finns inom den egna organisationen, är det viktigt att nyttiggöra informationen i samarbetet med andra brottsbekämpande organ. Ett

förbättrat informationsutbyte gör det möjligt att utnyttja de samlade resurserna effektivare och ökar förutsättningarna för att brott i större utsträckning och snabbare kan klaras upp och att felaktiga brottsmisstankar kan avföras från utredning.

Det pågår ett fortlöpande arbete med att utveckla system för informationsutbyte inom och mellan brottsbekämpande myndigheter, bl.a. inom ramen för det arbete som bedrivs av Rådet för rättsväsendets informationsförsörjning (där förutom polisen bl.a. Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Tullverket och Skatteverket ingår). Flera utredningar har också under senare år betonat att det måste skapas förutsättningar för ett förbättrat utbyte av information mellan de brottsbekämpande myndigheterna, se bl.a. SOU 2002:113, 2005:117 och 2006:18. Den gemensamma uppfattningen hos dessa utredningar har varit att en brottsbekämpande myndighet ska kunna lämna information till en annan sådan myndighet, om den senare myndigheten behöver informationen i sin brottsbekämpande verksamhet.

I avsnitt 7.2 berörs det myndighetsöverskridande arbetet mot organiserad brottslighet. I juli 2008 gav regeringen Rikspolisstyrelsen och andra berörda myndigheter i uppdrag att vidta åtgärder för att säkerställa en effektiv och uthållig bekämpning av den grova organiserade brottsligheten (dnr Ju2008/5776/PO). I uppdraget ingick att etablera ett antal regionala underrättelsecentrum och ett nationellt underrättelsecentrum. Uppdraget har redovisats i juni 2009 (dnr Ju 2009/5516/PO). Verksamheten förutsätter att information kan utbytas snabbt och enkelt. Bland de myndigheter som deltar i arbetet kan nämnas Kronofogdemyndigheten och Kriminalvården. Det innebär att samverkan går utanför kretsen av brottsbekämpande myndigheter. Frågan om informationsutbyte med andra myndigheter än brottsbekämpande behandlas i avsnitt 12.3.4.

Det är också en allmän strävan inom EU att öka informationsutbytet mellan medlemsstaternas brottsbekämpande myndigheter. I Europeiska rådets rekommendation om utarbetande av avtal mellan polis, tull och andra specialiserade brottsbekämpande organ, som antogs i april 2006 (6856/1/06 REV 1 ENFOCUSTOM 27 ENFOPOL 35 CRIMORG 40 CORDROGUE 15), betonar rådet vikten av ett förbättrat samarbete och informationsutbyte mellan de nationella brottsbekämpande myndigheterna.

Mot de fördelar som ett förbättrat informationsutbyte innebär ska ställas att ett ökat flöde av uppgifter mellan myndigheter kan skapa större risker för intrång i den personliga integriteten, särskilt som de uppgifter som polisen behandlar ofta är av känsligt slag. Även insamling och utbyte av förhållandevis harmlösa uppgifter kan, om de skapar en totalbild av en enskild persons förhållanden, riskera att leda till intrång i den personliga integriteten.

Vid informationsutbyte mellan brottsbekämpande myndigheter bör beaktas att de myndigheter som bedriver underrättelseverksamhet har likartade regler om sådan verksamhet och att alla myndigheter tillämpar samma grundläggande regler för brottsutredning. Vidare har uppgifter som rör brott och brottsbekämpning samma sekretesskydd hos alla berörda myndigheter. Skyddet vid personuppgiftsbehandling är också likartat. Även om det kan finnas nackdelar med ett ökat informationsflöde mellan de brottsbekämpande myndigheterna väger fördelarna över. De

integritetsrisker som kan finnas bör dock vägas in när bestämmelserna utformas och när myndigheter beviljas direktåtkomst.

Det ligger i sakens natur att informationsutbytet till stor del avser uppgifter som omfattas av sekretess, eftersom åtskilliga av de uppgifter som behandlas inom polisens brottsbekämpande verksamhet skyddas av någon typ av sekretess. En grundläggande förutsättning för att uppgifter ska få lämnas till en annan myndighet är att sekretess inte hindrar att uppgifterna lämnas ut. Detta gäller oberoende av om det rör sig om elektroniskt lagrade uppgifter eller uppgifter på papper. I offentlighets- och sekretesslagen (2009:400) finns ett antal bestämmelser som innebär att sekretess inte hindrar utbyte av uppgifter mellan nationella brottsbekämpande myndigheter.

Enligt 10 kap. 28 § offentlighets- och sekretesslagen finns det möjlighet att meddela sekretessbrytande föreskrifter i andra lagar och förordningar. I polisdatalagen (1998:622) och polisdataförordningen (1999:81) finns bestämmelser om utlämnande av uppgifter som har sekretessbrytande effekt. Frågan om sådana bestämmelser bör införas i den nya lagen behandlas i avsnitt 13.

Informationsutbytet mellan brottsbekämpande myndigheter sker framför allt manuellt. Uppgifter kan lämnas både i pappersform och elektroniskt, t.ex. via e-post. I viss utsträckning förekommer elektroniskt utlämnande genom att mottagaren ges rätt att själv söka efter information som den utlämnande myndigheten har tillgång till (direktåtkomst), men det gäller för närvarande bara uppgifter i vissa register.

En ordning som innebär att informationsutbytet i huvudsak sker genom manuell behandling skapar praktiska problem, särskilt som brottsbekämpningen bedrivs dygnet runt. Uppgifter som en tjänsteman behöver omedelbart för att kunna genomföra en tjänsteåtgärd måste vara lätt tillgängliga även utanför vanlig kontorstid. Direktåtkomst är således inte bara ett enkelt och arbetsbesparande sätt att lämna ut information utan ibland det enda i praktiken möjliga sättet att göra uppgifterna tillgängliga när de behövs.

Det finns ett stort och växande behov av effektivt informationsutbyte mellan de brottsbekämpande myndigheterna och detta behov måste kunna tillgodoses genom ökad användning av elektronisk kommunikation. Regeringen har i ett annat lagstiftningsärende framhållit att ett utökat elektroniskt informationsutbyte mellan myndigheter är ett nödvändigt steg i samhällets IT-utveckling (prop. 2007/08:160 s. 49). En ny lag bör således underlätta sådant informationsutbyte och bidra till att utveckla samarbetet med andra brottsbekämpande myndigheter, samtidigt som den värnar om enskildas integritet.

Samma begrepp som i annan likartad lagstiftning

Begreppet direktåtkomst har ingen legaldefinition. Den grundläggande innebörden av begreppet är att någon har direkt tillgång till någon annans register eller databaser och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen.

För annat elektroniskt utlämnande än genom direktåtkomst används begreppet utlämnande på medium för automatiserad behandling. Sådant

utlämnande kan innebära t.ex. att elektronisk information överförs via e-post, genom utlämnande av uppgifter på cd-rom, DVD, USB-minne eller genom direkt överföring från ett datorsystem till ett annat via allmänna kommunikationsnät.

Denna begreppsbildning, som används i många registerförfattningar, har kritiserats i olika sammanhang, vilket också de remissmyndigheter som är kritiska hänvisar till. Integritetsskyddsutredningen påpekar i sitt delbetänkande (SOU 2007:22, Del 1, s. 462 f.) att uttrycket direktåtkomst ibland, men inte alltid, avser utlämnande på elektroniskt medium. Vidare framhåller utredningen att det finns olika uppfattningar om huruvida bestämmelser om direktåtkomst är sekretessbrytande eller inte. Utredningens slutsats är att skyddet för den personliga integriteten skulle förbättras om regelverket var enhetligare och tydligare (s. 466).

Både från verksamhets- och integritetsperspektiv är det att föredra om de begrepp som används är tydliga och används på ett enhetligt sätt. I propositionen Utökat elektroniskt informationsutbyte diskuterar regeringen om begreppen direktåtkomst och utlämnande på medium för automatiserad behandling bör användas, mot bakgrund av remisskritik i det lagstiftningsärendet (prop. 2007/08:160 s. 58). Regeringen konstaterar där bl.a. att den tekniska utvecklingen har lett till att skillnaderna mellan direktåtkomst och utlämnande på medium för automatiserad behandling har blivit så liten att det ibland kan vara svårt att dra en gräns mellan dessa former av utlämnande. Regeringen uttalar vidare att mycket står att vinna med en mer enhetlig och tydlig begreppsbildning, men att den frågan inte bör lösas inom ramen för det enskilda lagstiftningsärendet.

Det är nödvändigt att reglera andra myndigheters tillgång till uppgifter i polisens brottsbekämpande verksamhet i den nya lagen, både därför att det kan förekomma ett relativt omfattande informationsutbyte med andra myndigheter och att polisen behandlar stora mängder information som uppfattas som känslig. Det skulle kunna leda till tolkningsproblem om man nu frångår den terminologi som används – eller har föreslagits – på närliggande områden. Det är vidare varken möjligt eller lämpligt att inom ramen för detta enskilda lagstiftningsärende avgöra den principiella frågan om vilken terminologi som bör användas i registerförfattningar. Mot den bakgrunden bör samma terminologi användas i den nya lagen som i annan likartad lagstiftning. Vidare bör uttrycket elektroniskt utlämnande användas som ett överordnat begrepp, som omfattar både direktåtkomst och utlämnande på medium för automatiserad behandling (se SOU 2007:64 s. 160; jfr prop. 2008/09:96 s. 8).

Frågor om direktåtkomst behandlas i avsnitt 12.3 och frågor om elektroniskt utlämnande på annat sätt i avsnitt 12.4. De föreslagna reglerna om direktåtkomst är inte sekretessbrytande.

12.2 Utgångspunkterna för informationsutbyte i det internationella samarbetet

Regeringens bedömning: Det internationella utbytet av information spelar en viktig roll för bekämpningen av framför allt allvarlig och gränsöverskridande brottslighet. Det arbetet bör kunna bedrivas i huvudsak på samma sätt som hittills.

Utredningen gör samma bedömning.

Remissinstanserna har inte haft någon invändning eller inte kommenterat saken närmare.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser kommenterar inte frågan. *Datainspektionen* påpekar att tillgänglighetsprincipen, som syftar till att förenkla informationsflödet mellan brottsbekämpande myndigheter inom EU, medför risk för att medlemsstaterna förlorar kontrollen över informationsflödet och att nationell lagstiftning inte längre räcker som instrument för att skydda informationen. Inspektionen efterlyser en detaljerad genomgång av de regler som motverkar integritetsintrång.

Skälen för regeringens bedömning: Av samma skäl som ett ökat informationsutbyte mellan svenska brottsbekämpande myndigheter bidrar till ett effektivare polisarbete gör internationellt samarbete i brottsbekämpande syfte det. Det är framför allt vid bekämpningen av allvarlig och gränsöverskridande brottslighet som det internationella informationsutbytet har betydelse. Utan sådant informationsutbyte skulle exempelvis bekämpningen av grov narkotikasmuggling, människohandel, penningtvätt och många andra typer av allvarliga brott inte kunna bedrivas lika effektivt. Dessutom har Sverige genom olika internationella överenskommelser åtagit sig att överlämna information som härrör från brottsbekämpande verksamhet dels till polismyndigheter i andra länder, dels till organisationer som Interpol och Europol. Hinder mot informationsutbyte på nationell nivå riskerar naturligtvis att påverka även det internationella informationsutbytet negativt. Det kan anmärkas att Sverige har ådragit sig kritik avseende informationsutbyte såväl nationellt som internationellt vid utvärdering av Europols verksamhet (se SOU 2005:117 s. 153).

Informationsutbytet inom EU bygger på principen om tillgänglighet. Den formuleras i Haagprogrammet från 2004 om förstärkt frihet, säkerhet och rättvisa i Europeiska unionen. Principen innebär att en tjänsteman, som sysslar med brottsbekämpning i en av unionens medlemsstater och som behöver information för att utföra sina uppgifter, ska kunna få denna från en annan medlemsstat som innehar informationen. Principen innebär också att de brottsbekämpande myndigheterna i den medlemsstat som har informationen ska göra denna tillgänglig.

Under senare år har det polisiära samarbetet mellan länderna inom EU utvecklats snabbt. Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater har genomförts genom förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen.

Syftet med rambeslutet är att få till stånd ett snabbare och enklare informationsutbyte, särskilt när det gäller allvarlig brottslighet. I avsnitt 4.4 redovisas även vissa andra EU-initiativ som syftar till att förbättra och förenkla informationsutbytet mellan medlemsstaterna.

Ett ökat informationsutbyte över gränserna måste emellertid balanseras av effektivt skydd för den enskilde bl.a. mot att uppgifterna används för andra syften. I december 2008 antogs rambeslutet om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet; EUT L 350, 30.12.2008, s. 60). Syftet med rambeslutet är att säkerställa en gemensam hög skyddsnivå för enskilda personer. Dataskyddsrambeslutet, som ska vara genomfört inom två år efter ikraftträdandet, innebär att det finns bindande förpliktelser om dataskydd mellan medlemsstaterna inom polisområdet. En redogörelse för rambeslutet finns i avsnitt 4.4.1.

Med anledning av *Datainspektionens* påpekande bör erinras om att många av de internationella överenskommelser som har tillkommit under senare år innehåller särskilda dataskyddsbestämmelser. Som exempel kan nämnas rådsbeslutet om inrättande av Europol (artiklarna 27–35), rådsbeslutet om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet, artiklarna 24–32), rambeslutet om förenklat informationsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen (artikel 8) och rambeslutet om utbyte av uppgifter ur kriminalregister (artikel 9). Inom vart och ett av dessa områden har man således tillskapat dataskyddsregler som är anpassade till det specifika informationsutbytet. Dessa regler kompletterar det generella skydd som Dataskyddsrambeslutet syftar till.

Det finns också anledning att i detta sammanhang framhålla att det polisiära samarbetet över gränserna i stor utsträckning sker som led i svenskt underrättelsearbete eller svensk förundersökning eller lagföring.

Sammantaget innebär utvecklingen att polisen kommer att ha ett fortsatt stort behov av att kunna utbyta uppgifter med andra länder. En ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör inte ställa upp onödiga hinder för sådant informationsutbyte. Möjligheterna att utbyta uppgifter bör i huvudsak motsvara vad som redan gäller. I avsnitt 12.3.5 diskuteras om utländska myndigheter bör kunna medges direktåtkomst till uppgifter i svenska register. I avsnitt 13.3 övervägs vilka sekretessbrytande bestämmelser om utlämnande som lagen bör innehålla. I det sammanhanget diskuteras det internationella informationsutbytet närmare.

12.3 Direktåtkomst

12.3.1 Regleringen av möjligheten till direktåtkomst

Regeringens förslag: Utlämnande genom direktåtkomst ska vara tillåtet enbart i den utsträckning som följer av den nya lagen.

Utredningen har inte behandlat frågan.
Remissinstanserna har inte berört frågan.

Promemorians förslag överensstämmer i sak med regeringens men innehåller inte något förslag om att möjligheten till direktåtkomst ska regleras uttömmande.

Remissinstanserna har inte tagit upp frågan.

Skälen för regeringens förslag: I polisdataförordningen (1999:81) finns bestämmelser om direktåtkomst till särskilda register hos polisen. Den nya lagen innebär att det krävs en mera generell reglering, eftersom lagen enbart sätter ramarna för behandlingen men inte, annat än i några specifika fall, anger vilka register som får föras. En generell reglering väcker i sin tur frågan om tillgången till uppgifter i polisens brottsbekämpande verksamhet genom direktåtkomst bör regleras uttömmande i den nya lagen.

Från integritetssynpunkt har det fördelar med en lösning där det i lagen framgår i vilken utsträckning direktåtkomst får medges. Det underlättar också för tillämparen att det anges i vilken utsträckning direktåtkomst kan förekomma. En särskild bestämmelse som anger att direktåtkomst ska vara tillåten enbart i den utsträckning det framgår av lagen bör därför införas.

12.3.2 De brottsbekämpande myndigheternas behov av direktåtkomst

Regeringens bedömning: Samtliga brottsbekämpande myndigheter har behov av att kunna få direktåtkomst till uppgifter som behandlas av polisen.

Utredningen berör inte frågan om övriga brottsbekämpande myndigheters allmänna behov av direktåtkomst till uppgifter som behandlas i polisens brottsbekämpande verksamhet.

Remissinstanserna: Flera remissinstanser, bl.a. dåvarande *Riksåklagaren,* dåvarande *Riksskatteverket, Tullverket* och *Kustbevakningen*, har påtalat att de har behov av att kunna ta del av uppgifter som behandlas i polisens brottsbekämpande verksamhet genom direktåtkomst.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna är genomgående positiva till promemorian i denna del och välkomnar bättre förutsättningar för informationsutbyte mellan de brottsbekämpande myndigheterna. De flesta av remissmyndigheterna har inte något att invända mot promemorians generella beskrivning av behovet av direktåtkomst.

Skälen för regeringens bedömning

Polisens nuvarande möjligheter att få direktåtkomst till uppgifter hos andra brottsbekämpande myndigheter

I promemorian finns en ingående redogörelse för såväl polisens möjlighet till och behov av tillgång genom direktåtkomst till uppgifter inom andra delar av polisverksamheten som andra brottsbekämpande myndigheters möjlighet till och behov av sådan tillgång till uppgifter hos polisen (Ds 2007:43 s. 201 f.).

Polisens möjlighet att ta del av uppgifter som behandlas hos andra brottsbekämpande myndigheter styrs genom de författningar som gäller för dessa myndigheter.

Beträffande uppgifter som behandlas av Tullverket föreskrivs i 6 § förordningen (2005:791) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet att Ekobrottsmyndigheten, Rikspolisstyrelsen, polismyndigheter, Kustbevakningen och Skatteverket får ha direktåtkomst till sådana uppgifter i tullbrottsdatabasen som behandlas för ändamålen att förhindra och upptäcka brottslig verksamhet. Enligt 7 § får Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och polismyndigheter ha direktåtkomst till sådana uppgifter som behandlas för ändamålen att utreda och beivra visst brott, om uppgifterna förekommer i en förundersökning som leds av åklagare.

Enligt 18 § förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen får övriga brottsbekämpande myndigheter ha direktåtkomst till uppgifter hos Kustbevakningen. För vissa myndigheter, dock inte polisen, är tillgången till uppgifter begränsad. I betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18) föreslås att Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, polismyndigheterna, Tullverket och Skatteverket ska kunna medges direktåtkomst till uppgifter som Kustbevakningen behandlar i sin brottsbekämpande verksamhet. Betänkandet, som har remissbehandlats, bereds inom Regeringskansliet (Försvarsdepartementet).

I betänkandet Åklagarväsendets brottsbekämpning Integritet – Effektivitet (SOU 2008:87) föreslås att Rikspolisstyrelsen, polismyndigheter, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till uppgifter i åklagarväsendets brottsbekämpande verksamhet. Betänkandet, som har remissbehandlats, bereds inom Regeringskansliet (Justitiedepartementet).

Andra myndigheters nuvarande möjligheter att få direktåtkomst till uppgifter som polisen behandlar

De övriga brottsbekämpande myndigheterna har redan i varierande utsträckning direktåtkomst till uppgifter som polisen behandlar i register.

Åklagarväsendet (Åklagarmyndigheten och Ekobrottsmyndigheten) har för närvarande direktåtkomst till misstankeregistret och belastningsregistret samt till uppgift om huruvida en person förekommer i DNA-register. I den polisiära verksamheten vid Ekobrottsmyndigheten har man direktåtkomst bl.a. till det centrala kriminalunderrättelseregistret och det allmänna spaningsregistret. Åklagarväsendet har också viss direktåtkomst till material i DurTvå vad avser förundersökningar som leds av åklagare.

Tullverket har direktåtkomst till misstankeregistret, belastningsregistret, Schengens informationssystem, beslags- och analysregister samt fingeravtrycks- och signalementsregister. Vidare har enskilda tulltjänstemän fått behörighet att ta del av vissa uppgifter i det allmänna spaningsregistret, godsregistret och registret över efterlysta fordon.

Kustbevakningen har direktåtkomst till Schengens informationssystem. Sedan den 1 juli 2009 kan Kustbevakningen, i likhet med övriga brotts-

bekämpande myndigheter, medges direktåtkomst till misstankeregistret och belastningsregistret (prop. 2008/09:152).

Skatteverket har direktåtkomst till misstankeregistret och belastningsregistret.

Ökade möjligheter till direktåtkomst behövs

I promemorian konstateras, något förenklat, att polismyndigheterna har behov av att få tillgång till varandras uppgifter, att Säkerhetspolisen har behov av att få tillgång till uppgifter som finns hos den övriga polisen, att åklagare har behov av framför allt tillgång till uppgifter i förundersökningar samt att Tullverket, Kustbevakningen och Skatteverket i sin brottsbekämpande verksamhet har varierande behov av tillgång både till uppgifter i förundersökningar och till underrättelseinformation.

Av de remissinstanser som uttalar sig i frågan bekräftar de flesta att andra brottsbekämpande myndigheter har ett uttalat behov av direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet.

Den brottsbekämpande verksamheten måste kunna bedrivas effektivt. Modern teknik ökar möjligheterna att skapa överblick och samordning i det brottsbekämpande arbetet och att utnyttja tillgänglig information på ett effektivt sätt. Det är angeläget att dessa möjligheter kan utnyttjas. En tjänsteman vid en myndighet som arbetar med en utredning eller något annat projekt som avser en misstänkt person eller viss misstänkt brottslig verksamhet bör på ett enkelt sätt kunna skaffa sig kunskap om existerande anmälningar och om huruvida det bedrivs brottsutredningar eller underrättelseprojekt riktade mot samma person eller samma företeelse av någon annan brottsbekämpande myndighet eller av samma myndighet i någon annan del av landet. De brottsbekämpande myndigheterna har därför ofta behov av att inte bara kunna på begäran få del av viss information utan att själva få omedelbar tillgång till denna genom direktåtkomst. För en sådan möjlighet talar också kostnads- och säkerhetsskäl. Det är inte kostnadseffektivt att myndigheter avsätter resurser för att manuellt administrera ett informationsutbyte när behovet av sådant utbyte kan konstateras redan på förhand. Utlämnande på annat sätt än genom direktåtkomst, exempelvis via fax eller e-post, innebär också allmänt sett ett mindre säkert överförande av uppgifter, eftersom obehöriga då lättare kan få tillgång till dem. Verksamhetsskäl talar således för att utöka de brottsbekämpande myndigheternas möjligheter till direktåtkomst.

Vittgående möjligheter till direktåtkomst ökar emellertid riskerna för intrång i den personliga integriteten. Typiskt sett innebär direktåtkomst att uppgifter blir tillgängliga för fler personer och att den ursprungliga myndighetens möjligheter att kontrollera användningen av uppgifterna minskar. Även om det är möjligt att genom särskilda åtgärder motverka dessa risker är det likväl viktigt att myndigheternas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna.

12.3.3 Direktåtkomst för svenska brottsbekämpande myndigheter

Regeringens förslag: Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket ska kunna medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen ska kunna medges direktåtkomst till register över DNA-profiler.

Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket ska kunna medges direktåtkomst till fingeravtrycks- eller signalementsregister.

Säkerhetspolisen ska kunna medges direktåtkomst i samma utsträckning som gäller för Rikspolisstyrelsen i övrigt och för polismyndigheter.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag: Polismyndigheter ska få ha direktåtkomst till det allmänna spaningsregistret och Statens kriminaltekniska laboratorium, polismyndigheter och åklagarmyndigheter ska få ha direktåtkomst till register med DNA-analyser i brottmål. Direktåtkomst till personuppgifter ska förbehållas de personer inom polisen som på grund av sina arbetsuppgifter behöver tillgång till uppgifterna.

Remissinstanserna: Flera myndigheter, bl.a. dåvarande *Riksåklagaren*, dåvarande *Riksskatteverket*, *Tullverket* och *Kustbevakningen*, har ansett att deras respektive myndigheter bör kunna medges direktåtkomst till uppgifter som behandlas i polisens brottsbekämpande verksamhet.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår dock inte att Tullverket och Kustbevakningen ska kunna få direktåtkomst till uppgifter i register över DNA-profiler.

Remissinstanserna: *Åklagarmyndigheten* och *Ekobrottsmyndigheten* lyfter fram åklagarväsendets behov av att få direktåtkomst till underrättelseinformation, men har inga invändningar mot utformningen av förslaget. *Rikspolisstyrelsen* menar att åklagarväsendets tillgång till underrättelseinformation är en principiellt viktig fråga som bör diskuteras vidare men att man bör avvakta bl.a. Insynsutredningens arbete innan slutlig ställning tas. *Skatteverket* vänder sig mot att det ska vara en förutsättning för direktåtkomst att uppgifterna har gjorts gemensamt tillgängliga hos polisen.

När det gäller tillgången till de register som föreslås regleras särskilt anser *Statens kriminaltekniska laboratorium* att Tullverket och Kustbevakningen, på samma sätt som bl.a. åklagare, bör kunna medges direktåtkomst till uppgifter om huruvida en person förekommer i register över DNA-profiler, eftersom det skulle effektivisera samarbetet. *Tullverket* efterfrågar inte direktåtkomst till register över DNA-profiler men däremot information om huruvida en person tidigare har fått lämna DNA-prov enligt bestämmelserna i 28 kap. 12 a § rättegångsbalken. *Eko-*

brottsmyndigheten anser att både myndigheten och polismyndigheterna bör få tillgång till uppgifter i penningtvättsregister.

Skälen för regeringens förslag

I vilken utsträckning bör andra brottsbekämpande myndigheter kunna medges direktåtkomst?

I föregående avsnitt har konstaterats att andra brottsbekämpande myndigheter behöver ha direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet. I nästa avsnitt diskuteras frågan om, och i så fall i vilken utsträckning, myndigheter som biträder eller samarbetar med polisen, men som inte direkt har brottsbekämpande uppgifter, bör kunna medges direktåtkomst.

Mot de brottsbekämpande myndigheternas verksamhetsbehov måste hänsynen till enskildas integritet vägas. Integritetsaspekterna måste tillmätas central betydelse vid bedömningen av i vilken omfattning sådana myndigheter bör kunna medges direktåtkomst till uppgifter i varandras verksamhet. I de databaser och register som förs av brottsbekämpande myndigheter finns det ofta stora mängder personuppgifter. Många av dessa kan vara av känslig karaktär. Enbart det förhållandet att uppgifter om en enskild persons förhållanden samlas in och bevaras kan uppfattas som ett intrång i den personliga integriteten. Ju fler personer som har omedelbar tillgång till sådana uppgiftssamlingar, desto mera påtaglig är risken för intrång. Direktåtkomst kan också minska möjligheterna att kontrollera den vidare användningen av uppgifterna. Dessa förhållanden utgör skäl för en restriktiv hållning i fråga om direktåtkomst till uppgifter som polisen behandlar.

En viktig aspekt som bör beaktas vid den avvägning som måste göras är om det, när det är fråga om direktåtkomst till sekretessreglerade uppgifter, gäller sekretess för uppgifterna hos den mottagande myndigheten. En annan viktig aspekt är hur uppgifterna sprids och används inom den mottagande myndigheten. Om användandet av uppgifterna inom den myndigheten kan begränsas till en liten krets, är integritetsriskerna mindre än om uppgifterna ges en vid spridning. En tredje aspekt är vilka bestämmelser om informationssäkerhet (exempelvis system för behörighet, loggning och tillsyn) som gäller hos den mottagande myndigheten. Om informationssäkerheten hos den mottagande myndigheten är hög, så att det kan garanteras att informationen endast når dem som har behov av den, inger möjlighet till direktåtkomst mindre betänkligheter från integritetssynpunkt än vad som annars hade varit fallet.

Inledningsvis kan anmärkas att de brottsbekämpande myndigheterna har författningar som reglerar personuppgiftsbehandlingen på ett likartat sätt. Sekretessregleringen ger också i princip samma skydd för uppgifter i brottsbekämpningen hos samtliga brottsbekämpande myndigheter. Myndigheterna omfattas således av bl.a. bestämmelserna om skydd för brottsbekämpningen i 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen och bestämmelserna om skydd för enskildas personliga och ekonomiska förhållanden i sådan verksamhet, som regleras i 35 kap. samma lag. Numera finns det också en särskild bestämmelse, 11 kap. 4 §, om överföring av sekretess vid direktåtkomst. Om en myndighet har elektro-

nisk tillgång till en annan myndighets upptagning för automatiserad behandling och en uppgift i denna upptagning är sekretessreglerad hos den andra myndigheten, blir sekretessbestämmelsen tillämplig också hos den mottagande myndigheten. Detta gäller dock inte om uppgiften ingår i ett beslut hos den mottagande myndigheten. Det finns även en särskild bestämmelse om vad som gäller vid konkurrens mellan den överförda sekretessen och sådan sekretess som är direkt tillämplig hos den mottagande myndigheten, 11 kap. 8 § offentlighets- och sekretesslagen, se avsnitt 13.1.

Vad sedan gäller tillgången till uppgifterna hos de mottagande myndigheterna har i avsnitt 6.6 föreslagits att en enskild tjänsteman inom polisväsendet ska ges tillgång endast till sådana uppgifter som han eller hon behöver för att kunna fullgöra sina arbetsuppgifter på ett ändamålsenligt sätt. Motsvarande begränsning bör gälla hos de myndigheter som genom direktåtkomst får tillgång till personuppgifter som polisen behandlar. Särskilda regler om detta bör införas i den nya lagen. En möjlighet till direktåtkomst behöver alltså inte innebära att annat än en begränsad krets av tjänstemän – eller enbart en viss tjänsteman – hos den mottagande myndigheten får tillgång till uppgifterna.

Vad slutligen gäller informationssäkerhet i samband med direktåtkomst har regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela särskilda föreskrifter om detta. Om de brottsbekämpande myndigheterna ska ges möjlighet till direktåtkomst till varandras uppgifter, bör den myndighet som beslutar om sådan åtkomst vara skyldig att försäkra sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå, exempelvis vad gäller system för utlämnande av behörighet och loggning av transaktioner samt tillsyn. Det kan i sammanhanget noteras att den tekniska utvecklingen fortlöpande ger bättre möjligheter att begränsa tillgången till olika uppgifter och att i efterhand genom bl.a. loggningsuppgifter kontrollera hur tillgången har utnyttjats. Ett av syftena med den nya tekniska struktur för lagring av personuppgifter som planeras av polisen är att göra det lättare att begränsa tillgången på detta sätt.

De ökade integritetsrisker som en möjlighet till direktåtkomst kan medföra kan alltså motverkas genom bestämmelser av annat slag, såsom befintliga bestämmelser om sekretess hos den mottagande myndigheten och bestämmelser om tillgång till uppgifter och om informationssäkerhet. Övervägande skäl talar därför för att den nya lagen bör tillåta att övriga brottsbekämpande myndigheter ges direktåtkomst till personuppgifter som behandlas i polisens brottsbekämpande verksamhet. De närmare förutsättningarna för sådan direktåtkomst diskuteras i det följande.

Hur bör direktåtkomsten till polisens uppgifter avgränsas?

En första fråga är om det, för att en myndighet ska kunna ges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet, bör krävas att uppgifterna är gemensamt tillgängliga hos polisen. *Skatteverket* anser att detta inte bör vara en förutsättning för direktåtkomst. Enligt verket bör det vara möjligt att arbeta i mindre myndighetsöverskridande projekt utan att uppgifterna därigenom blir gemensamt tillgängliga. Även om myndighetsöverskridande samarbete äger rum i mindre grupper innebär

informationsutbytet att uppgifter som behandlas av polisen blir tillgängliga utanför det sammanhang där de ursprungligen har behandlats. Det är då ur ett integritetsperspektiv rimligt att de särskilda, mer begränsande, reglerna om gemensamt tillgängliga uppgifter alltid tillämpas. Direktåtkomst bör således endast medges för uppgifter som är gemensamt tillgängliga.

En ytterligare förutsättning för att direktåtkomst ska kunna medges bör vara att den myndighet som beslutar om sådan åtkomst försäkrar sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå. *Rikspolisstyrelsen* betonar vikten av att det tydligt framgår att det är polisen som avgör om uppgifter bör lämnas ut till en annan myndighet i denna form. *Ekobrottsmyndigheten* anser däremot att det bör ankomma på någon annan myndighet än polisen, exempelvis Datainspektionen, att avgöra om en myndighet uppfyller acceptabla krav på säkerhetsnivå för att kunna medges direktåtkomst, eftersom myndigheter inte bör ha kontrollskyldighet i förhållande till varandra. Det bör, som Rikspolisstyrelsen anför, vara den myndighet som ansvarar för datasystemen som avgör i vilken utsträckning en annan myndighet kan anses tillgodose kraven på tillräcklig datasäkerhet. Den som medger direktåtkomst ska kunna ha kontroll över att det egna datasystemet alltjämt har tillräcklig datasäkerhet även efter det att andra myndigheter fått tillgång till detta. Den närmare bedömningen av tekniska och andra förutsättningar för direktåtkomst måste därför göras av polisen.

En annan förutsättning bör vara att en enskild tjänsteman ska få ha direktåtkomst endast till sådana uppgifter som han eller hon behöver för att kunna fullgöra sina arbetsuppgifter på ett ändamålsenligt sätt. De närmare förutsättningarna för detta regleras lämpligen i förordning eller genom myndighetsföreskrifter.

I promemorian diskuteras ingående om det bör införas ytterligare begränsningar i möjligheten till direktåtkomst t.ex. enbart till visst register, viss uppgiftssamling eller viss brottstyp (Ds 2007:43 s. 221 f.). Slutsatsen är att det varken är önskvärt eller möjligt att i den nya lagen uppställa andra begränsningar vad gäller de brottsbekämpande myndigheternas direktåtkomst än de behörighets- och behovsbegränsningar som angetts ovan. Remissinstanserna framför inga synpunkter på detta och det finns inte skäl att nu göra en annan bedömning.

I avsnitt 13 behandlas frågan om huruvida sekretess hindrar direktåtkomst.

Direktåtkomst till uppgifter hos Säkerhetspolisen och till vissa särskilda register

Som tidigare har angetts bör vissa register undantas från den nya lagens tillämpningsområde, bl.a. belastningsregistret och misstankeregistret. De lagar som reglerar dessa register innehåller särskilda bestämmelser om direktåtkomst. Frågan om direktåtkomst till de registren bör därför inte regleras i den nya lagen.

I fråga om de register som föreslås regleras särskilt i den nya lagen och behandlingen av personuppgifter hos Säkerhetspolisen görs följande bedömning.

Eftersom Säkerhetspolisen behandlar särskilt känsliga uppgifter föreslås i promemorian att det inte ska vara möjligt att medge direktåtkomst till uppgifter som behandlas där. Några skäl att införa en möjlighet till direktåtkomst har inte framkommit under remissbehandlingen. Endast Säkerhetspolisens egna tjänstemän bör således kunna ges direkt tillgång till uppgifterna.

I avsnitt 15.4 behandlas penningtvättsregister, som i stor utsträckning innehåller underrättelseinformation. Denna underrättelseinformation är till sin natur sådan att det är viktigt att tillgången till den begränsas till ett fåtal personer. *Ekobrottsmyndigheten* menar att det skapar problem att myndigheten och Finanspolisen inte har tillgång till varandras databaser. Samma skäl som talar för att Finanspolisen ska kunna medges direktåtkomst till uppgifter som behandlas vid Ekobrottsmyndigheten och andra polismyndigheter talar enligt Ekobrottsmyndigheten för att dessa myndigheter ska kunna få direktåtkomst till penningtvättsregister.

Penningtvättsregister innehåller känslig ekonomisk information och speciell underrättelseinformation, som enligt gällande regler inte är åtkomlig ens för andra delar av polisorganisationen. Det är i stor utsträckning fråga om obearbetad information, som mottagits från finanssektorn som ett resultat av vissa företags rapporteringsskyldighet. Uppgifterna får registreras innan någon analys av uppgifternas relevans ur brottsbekämpningsperspektiv ännu har gjorts. Värdet av sådant underrättelsematerial är svårt att bedöma utan tillgång till specialkunskaper. Vidare får penningtvättsregister innehålla uppgifter om misstänkt finansiering av terrorism. I linje med att direktåtkomst inte föreslås kunna ges till de uppgifter som Säkerhetspolisen behandlar, bör direktåtkomst inte heller kunna medges till uppgifter som behandlas med anledning av misstänkt penningtvätt eller misstänkt finansiering av terrorism.

När det gäller register över DNA-profiler (DNA-registret, utredningsregistret och spårregistret) bör enligt promemorian de myndigheter som redan har rätt till direktåtkomst, dvs. polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten och Statens kriminaltekniska laboratorium (11 § polisdataförordningen), kunna medges direktåtkomst. För polismyndigheter och åklagarmyndigheter bör enligt promemorian åtkomsten, på samma sätt som nu, begränsas till uppgifter om huruvida en person förekommer i registret eller inte, vilket regeringen bör meddela föreskrifter om. Remissinstanserna lämnar inga synpunkter på dessa myndigheters tillgång till registren. Förslaget bör genomföras. Frågan om Statens kriminaltekniska laboratorium ska ha direktåtkomst till registren behandlas i avsnitt 12.3.4.

Varken Tullverket eller Kustbevakningen uttrycker något behov av att få direktåtkomst till register över DNA-profiler. *Tullverket* efterlyser däremot information om huruvida en person tidigare har fått lämna DNA-prov. Enligt 28 kap. 12 a § rättegångsbalken kan salivprov tas rutinmässigt på den som är skäligen misstänkt för brott av viss svårhetsgrad. Tullverket tar upp en fråga som är viktig både från effektivitetssynpunkt och integritetssynpunkt, nämligen hur man ska säkerställa att det inte tas upprepade salivprov på en person som redan underkastats provtagning. Själva provtagningen registreras inte men däremot utfallet av provet, om bestämmelserna i polisdatalagen medger det. I den mån personen är registrerad i DNA-registret eller utredningsregistret behöver

något nytt prov normalt inte tas. Mot den bakgrunden ter det sig rimligt att Tullverket, som i stor utsträckning ingriper mot brott för vilka straffskalan är sådan att DNA-prov kan aktualiseras, bör kunna medges tillgång till samma information som åklagare, nämligen om huruvida en viss person förekommer i register över DNA-profiler. Sådan information innebär att man kan undvika att onödiga DNA-prov tas. Vad som nu har sagts om Tullverkets behov gäller i princip även för Kustbevakningen. För närvarande är Kustbevakningens möjligheter att ingripa mot brott som ger möjlighet att ta DNA-prov begränsade, men den har utökats under senare tid. I betänkandet Kustbevakningens rättsliga befogenheter (SOU 2008:55) föreslås att myndigheten ska kunna inleda och bedriva förundersökning beträffande betydligt fler brottstyper som ger grund för att ta DNA-prov. Betänkandet, som har remissbehandlats, bereds för närvarande i Regeringskansliet (Försvarsdepartementet). Mot den nu angivna bakgrunden finner regeringen att den nya lagen bör öppna möjlighet att ge även Kustbevakningen direktåtkomst till register över DNA-profiler. Genom detta tillgodoses *Statens kriminaltekniska laboratoriums* synpunkter. Samma begränsning av tillgången till uppgifter som för närvarande gäller för polismyndigheter och åklagare bör gälla för Tullverket och Kustbevakningen.

När det gäller tillgången till uppgifter i fingeravtrycks- eller signalementsregister framför remissinstanserna inga synpunkter på promemorians förslag. Eftersom det finns ett stort behov av att snabbt kunna få tillgång till sådana uppgifter i identifieringssyfte bör, som föreslås i promemorian, samtliga brottsbekämpande myndigheter med undantag för åklagare kunna medges direktåtkomst till personuppgifter i registren i fråga. I avsnitt 12.3.4 behandlas frågan om Statens kriminaltekniska laboratorium ska kunna medges direktåtkomst.

Då promemorian inte innehåller något förslag om register för handläggningen av internationella ärenden har frågan om direktåtkomst till det registret inte aktualiserats. Registret har framför allt till syfte att underlätta Rikspolisstyrelsens verksamhet som mottagare och förmedlare av information. Uppgifterna i registret är knappast av intresse för andra myndigheter i deras brottsbekämpande arbete. Några verksamhetsskäl som kan motivera att andra brottsbekämpande myndigheter skulle ges tillgång till registret har inte framkommit. Både integritetsskäl och verksamhetsskäl talar mot att tillåta direktåtkomst till registret. Dels kan en utländsk myndighet ha ålagt svenska myndigheter att iaktta begränsningar i spridningen av uppgifterna, dels kan det vara svårt för andra tjänstemän än de som sysslar med internationella frågor att bedöma värdet av uppgifterna. Mot den bakgrunden bör det inte införas någon möjlighet till direktåtkomst till uppgifter i det internationella registret.

12.3.4 Direktåtkomst för andra svenska myndigheter

Regeringens förslag: Statens kriminaltekniska laboratorium ska kunna medges direktåtkomst till register över DNA-profiler och till fingeravtrycks- eller signalementsregister.

Regeringens bedömning: Andra myndigheter som inte är brottsbekämpande bör inte kunna medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet.

Utredningen behandlar inte frågan.

Remissinstanserna har inte haft några synpunkter.

Promemorian föreslår att Statens kriminaltekniska laboratorium ska kunna medges direktåtkomst till register över DNA-profiler och till fingeravtrycks- eller signalementsregister men tar inte upp frågan om direktåtkomst för andra myndigheter.

Remissinstanserna: *Rikspolisstyrelsen* påpekar att Kronofogdemyndigheten, Försäkringskassan och Skatteverkets fiskala del deltar i verksamheten vid regionala underrättelsecentrum, där även Kriminalvården och Migrationsverket är representerade. I det fortsatta arbetet bör enligt styrelsen övervägas om inte även dessa myndigheter ska kunna medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet. *Statens kriminaltekniska laboratorium* anser att den nya lagen ska gälla även för laboratoriet. *Kronofogdemyndigheten* menar att det finns skäl att överväga utökade möjligheter till informationsutbyte även med myndigheter som inte är direkt brottsbekämpande och pekar på det samarbete som myndigheten bedriver på lokal och central nivå för att motverka grov och organiserad brottslighet. *Kriminalvården* pekar bl.a. på myndighetens uppgift att förhindra återfall i brott. Myndigheten menar att man har en brottsbekämpande roll och att det finns starka skäl att utvidga möjligheterna att utbyta information mellan Kriminalvården och polisen. *Finansinspektionen* anser sig inte ha behov av tillgång till uppgifter i penningtvättsregister, men önskar information om företagens förmåga att rapportera misstänkt penningtvätt.

Skälen för regeringens förslag och bedömning

Statens kriminaltekniska laboratoriums tillgång till vissa register

I avsnitt 6.3 har tanken på att lagen ska gälla även för *Statens kriminaltekniska laboratorium* avvisats. Myndigheten har dock behov av direktåtkomst till vissa av de register som enligt förslagen i avsnitt 15 ska regleras särskilt i den nya lagen. Ingen av remissinstanserna har ifrågasatt detta. Myndigheten hanterar redan nu registren med DNA-profiler (DNA-registret, utredningsregistret och spårregistret) i egenskap av personuppgiftsbiträde åt Rikspolisstyrelsen. Denna hantering förutsätter att laboratoriet har direktåtkomst till registren, vilket regleras i 11 § polisdataförordningen. Vidare utför Statens kriminaltekniska laboratorium analyser av fingeravtryck för polisens räkning och behöver av det skälet på samma sätt som nu direktåtkomst till fingeravtrycks- eller signalementsregister. Bestämmelser om att Statens kriminaltekniska laborato-

rium ska kunna medges direktåtkomst till nämnda register bör därför införas.

Bör andra myndigheter kunna medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet?

Det allmänna myndighetsöverskridande samarbetet för att förebygga och bekämpa brott utvecklas fortlöpande. Ett viktigt inslag i detta är uppdraget till Rikspolisstyrelsen och andra berörda myndigheter att vidta åtgärder för att säkerställa en effektiv och uthållig bekämpning av grov organiserad brottslighet (se avsnitt 7.2). Informationsutbyte är en grundläggande beståndsdel i detta arbete, som även involverar myndigheter som inte är brottsbekämpande. Frågan är om detta samarbete motiverar att kretsen av myndigheter som får medges direktåtkomst vidgas utöver vad som föreslås i promemorian, eller om informationsbehovet kan tillgodoses på annat sätt.

Det är, som utvecklats tidigare, viktigt med ett närmare samarbete och ökat informationsutbyte mellan Kriminalvården och polisen för att förebygga brott. Detta markeras genom den utvidgning av lagens sekundära ändamål som föreslås i avsnitt 7.6. Enligt förslaget ska personuppgifter som behandlas i polisens brottsbekämpande verksamhet även få behandlas när det är nödvändigt för att tillhandahålla information som behövs i verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten. I samma avsnitt föreslås att ett annat sekundärt ändamål ska vara att behandla uppgifter för att tillhandahålla dessa till myndigheter som inte är brottsbekämpande, om tillhandahållandet sker i syfte att samverka mot brott. De synpunkter som *Kriminalvården* och *Kronofogdemyndigheten* framför får därmed anses tillgodosedda.

Rikspolisstyrelsen anser att det bör övervägas att ge vissa myndigheter, som inte är brottsbekämpande, direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet. Regeringen vill understryka betydelsen av det samarbete som förekommer mellan polisen och myndigheter som inte är brottsbekämpande. Samarbetet kommer sannolikt att utvecklas ytterligare i framtiden. Samtidigt har detta samarbete inte samma frekvens och intensitet som exempelvis samarbetet mellan polisen och åklagare, möjligen med undantag för situationer där man i någon form bedriver verksamhet tillsammans i gemensamma lokaler. Verksamhetsintressena av direktåtkomst är därför inte lika starka som när det gäller brottsbekämpande myndigheter. Härtill kommer att det hos myndigheter utanför kretsen av brottsbekämpare kan gälla andra sekretessregler och andra krav på insyn i verksamheten.

Eftersom direktåtkomst innebär ökad risk för integritetsintrång väger integritetsintressena i detta fall tyngre än önskemålen om utökad direktåtkomst. Det finns således inte skäl att nu föreslå att någon ytterligare myndighet utanför de brottsbekämpande ska kunna få tillgång till uppgifter i polisens brottsbekämpande verksamhet genom direktåtkomst.

Både *Skatteverket* och *Finansinspektionen* tar upp frågan om tillgång till annan information om penningtvätt än den som finns penningtvättsregister. Den frågan behandlas i avsnitt 15.4.

12.3.5 Direktåtkomst för utländska myndigheter

Regeringens förslag: Regeringen ska få meddela föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet. Förutsättningen ska vara att detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller att det följer av en EU-rättsakt.

Utredningen behandlar inte frågan.

Remissinstanserna har inte yttrat sig i saken.

Promemorians förslag överensstämmer delvis med regeringens. Beträffande DNA-register och fingeravtrycks- eller signalementsregister föreslås att regeringen får meddela föreskrifter om att en utländsk myndighet får medges direktåtkomst i den utsträckning detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Promemorian innehåller inte något förslag om direktåtkomst för Europol eller mellanfolkliga organisationer.

Remissinstanserna: Remissinstanserna godtar i allmänhet förslaget. *Datainspektionen* efterlyser en redogörelse för hur integritetsskyddsaspekter tillgodoses vid direktåtkomst för utländska myndigheter. Enligt inspektionen torde Prümrådsbeslutet, som förutsätter direktåtkomst till avidentifierade uppgifter, förutsätta viss ändring i förslaget. *Lunds Universitet* vänder sig mot att regeringen får en omfattande delegation när det gäller direktåtkomst för utländska myndigheter och förordar lagreglering.

Skälen för regeringens förslag: Numera finns så gott som all polisiär information i automatiserad form. Det aktualiserar frågan om elektronisk informationsöverföring till andra stater. Utlämnande genom direktåtkomst för utländska myndigheter till uppgifter som behandlas av polisen har hittills endast aktualiserats i ett fall.

Nyligen antogs Europeiska rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, Prümrådsbeslutet. Beslutet innehåller bl.a. bestämmelser som ålägger medlemsstaterna att tillåta direktåtkomst till vissa uppgifter i nationella DNA-register och fingeravtrycksregister. Åtkomsten ska begränsas till uppgifter om huruvida någon förekommer i registren eller inte. Prümrådsbeslutet innehåller särskilda dataskyddsregler (artiklarna 24–32). Som framgår av avsnitt 4.4.3 har riksdagen godkänt rådsbeslutet.

Eftersom det föreslås att det ska följa av den nya lagen i vilken utsträckning direktåtkomst ska vara tillåten (avsnitt 12.3.1) behövs det en bestämmelse om direktåtkomst för utländsk myndighet. Eftersom man kan förutse en fortsatt utveckling av informationsutbytet framför allt inom EU bör bestämmelsen inte knytas enbart till den överenskommelse som finns nu utan göras generell.

Lunds universitet har invänt att promemorians förslag innebär en alltför omfattande delegation till regeringen. I många registerförfattningar regleras grundläggande frågor i lag, bl.a. möjligheten att bevilja direktåtkomst, medan närmare förutsättningar för direktåtkomst ofta regleras i förordning. I de fall där riksdagen har tagit ställning till frågan om att

tillåta en utländsk myndighet direktåtkomst, genom att godkänna en internationell överenskommelse, är det enligt regeringens mening rimligt att de närmare bestämmelserna om direktåtkomsten kan beslutas av regeringen.

Om direktåtkomst till vissa uppgifter i framtiden skulle komma att regleras i EU-rättsakter som inte kräver riksdagens godkännande framstår det som naturligt med en bestämmelse som kan täcka behovet av reglering av detaljfrågor även i sådana fall.

Den i promemorian föreslagna bestämmelsen tar sikte enbart på direktåtkomst för utländska myndigheter. Mot bakgrund av att polissamarbetet i stor utsträckning äger rum genom mellanfolkliga organisationer bör bestämmelsen även omfatta direktåtkomst för mellanfolkliga organisationer som är brottsbekämpande, om det finns en bindande internationell överenskommelse om det.

Datainspektionen tar upp frågan om hur integritetsskyddet ska säkras om utländska myndigheter ges direktåtkomst till svensk information. Inspektionen framhåller att tillgänglighetsprincipen medför en risk att medlemsstaterna förlorar kontrollen över informationsflödet och att nationell lagstiftning inte längre räcker som instrument för att skydda informationen. Här finns anledning att erinra om att möjligheten till direktåtkomst för utländska myndigheter hittills enbart aktualiserats beträffande vissa typer av uppgifter i några av de register som regleras särskilt i den nya lagen, nämligen register över DNA-profiler och fingeravtrycksregister. Direktåtkomsten ska inte omfatta uppgifter som avslöjar personens identitet. För att få ytterligare information måste den andra staten ansöka om rättslig hjälp i Sverige. Vidare innehåller Prümrådsbeslutet särskilda regler som syftar bl.a. till att säkerställa informationens korrekthet och aktualitet. Reglerna anger hur och av vem uppgifterna får användas samt tillförsäkrar berörda personer rätt till information och skadestånd. Integritetsskyddande bestämmelser finns således. När det gäller eventuella framtida överenskommelser inom EU säkerställer dataskyddsrambeslutet en hög skyddsnivå vid behandlingen av personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna.

12.4 Elektroniskt utlämnande på annat sätt än genom direktåtkomst

Regeringens förslag: Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen har möjlighet att meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall.

Utredningen lämnar inte något förslag om utlämnande av uppgifter på medium för automatiserad behandling.

Remissinstanserna har inte uttalat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Bestämmelsen om utlämnande på medium för automatiserad behandling kritiseras från olika utgångspunkter av *Rikspolisstyrelsen*, *Säkerhetspolisen, Statens kriminaltekniska laboratorium,*

Skatteverket, Kronofogdemyndigheten, Sveriges advokatsamfund och *Journalistförbundet*. Flera av dessa kritiserar användningen av begreppet utlämnande på medium för automatiserad behandling. Flertalet anser att regleringen är otidsenlig och att man skapar onödiga begränsningar i informationsutbytet mellan brottsbekämpande myndigheter. Journalistförbundet anser att bestämmelsen strider mot offentlighetsprincipen. Förbundet efterlyser också en proportionalitetsavvägning mellan skyddet för den personliga integriteten och förbudet mot att använda viss teknik.

Både *Rikspolisstyrelsen* och *Säkerhetspolisen* efterlyser klarlägganden om vilket uppgiftslämnande som är tillåtet på medium för automatiserad behandling. Rikspolisstyrelsen pekar på att det förekommer ett omfattande informationsutbyte både inom och utom landet vid såväl brottsutredningar som underrättelsearbete och att det kan krävas undantag i förordning för information till Interpol och Europol. Säkerhetspolisen framhåller att man måste kunna få stora mängder uppgifter från den övriga polisen överförda elektroniskt i samband med registerkontroll för säkerhetsprövning.

Skälen för regeringens förslag: Uppgifter kan lämnas ut från polisen i elektronisk form på medium för automatiserad behandling, bl.a. genom e-post eller genom direkt överföring från ett datasystem till ett annat via allmänna kommunikationsnät. Inte bara direktåtkomst utan även utlämnande av personuppgifter på medium för automatiserad behandling anses medföra särskilda 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 riskerna för att uppgifterna ska behandlas i strid med de grundläggande kraven på dataskydd. Utlämnande i elektronisk form skapar också möjlighet för myndigheterna att inrätta rutiner som innefattar dagliga överföringar av större mängder av uppgifter via t.ex. e-post. Även om direktåtkomst generellt får betraktas som den mest känsliga formen av elektroniskt utlämnande kan i vissa fall likartade risker föreligga vid andra former av elektroniskt utlämnande. Med hänsyn härtill föreslås i promemorian att förutsättningarna för utlämnande av personuppgifter på medium för automatiserad behandling författningsregleras.

Journalistförbundet ifrågasätter om en bestämmelse av detta slag är förenlig med offentlighetsprincipen. Bestämmelsen påverkar inte rätten att få ta del av allmänna handlingar utan endast i vilken form handlingarna får göras tillgängliga. Vidare finns det inte någon i lag föreskriven skyldighet att lämna ut handlingar elektroniskt som är relevant i detta sammanhang (jfr 2 kap. 13 § tryckfrihetsförordningen). Offentlighetsprincipen utgör således inget hinder mot en bestämmelse av det aktuella slaget. Motsvarande bestämmelser finns i andra registerlagar, exempelvis lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

E-offentlighetskommittén (Ju 2008:06) utreder frågan om det ska införas en skyldighet, generellt eller i begränsad utsträckning, att lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form (dir. 2008:26). Om en sådan skyldighet införs kan bestämmelser i olika registerlagar, bl.a. den nu föreslagna lagen, behöva ses över.

Regeringen delar promemorians bedömning att huvudregeln bör vara att bara enstaka uppgifter får lämnas ut på medium för automatiserad behandling, t.ex. genom e-post, när förutsättningarna för ett utlämnande i övrigt är uppfyllda. Detta överensstämmer med vad som redan gäller bl.a. för Tullverkets brottsbekämpande verksamhet och som föreslås för åklagarväsendets och Kustbevakningens personuppgiftsbehandling. Kritiken mot användningen av begreppet utlämnande på medium för automatiserad behandling bemöts i avsnitt 12.1.

I förhållande till myndigheter som får medges direktåtkomst bör det dock inte gälla några begränsningar i fråga om utlämnande på annat elektroniskt medium, med hänsyn till att lagen ska vara teknikneutral. Regeringen avser att i förordning meddela föreskrifter om detta. Med en sådan lösning tillgodoses de synpunkter som bl.a. *Rikspolisstyrelsen*, *Säkerhetspolisen, Statens kriminaltekniska laboratorium* och *Skatteverket* framför. När det gäller utlämnande till andra myndigheter bör regeringen också ha möjlighet att i förordning medge sådant elektroniskt utlämnande.

Regeringen bör vidare ha möjlighet att i förordning medge utlämnande på medium för automatiserad behandling även i andra fall. Som exempel kan nämnas utlämnande av en förundersökning eller annan utredning enligt bestämmelserna i 23 kap. rättegångsbalken till försvarare eller annat juridiskt biträde. Behovet av att kunna använda elektronisk överföring vid informationsutbytet med Interpol och Europol, som *Rikspolisstyrelsen* lyfter fram, kan också lösas på detta sätt.

13 Sekretess och uppgiftsskyldighet

13.1 Allmänna utgångspunkter

Regeringens bedömning: Det behövs sekretessbrytande regler för att skapa förutsättningar för ett bättre informationsutbyte.

Utredningen diskuterar inte frågan på ett generellt plan.

Remissinstanserna: Flera remissinstanser, däribland dåvarande *Riksåklagaren,* dåvarande *Riksskatteverket, Tullverket* och *Kustbevakningen*, har ifrågasatt varför utredningen inte i större utsträckning har beaktat behovet av informationsutbyte mellan brottsbekämpande myndigheter.

Promemorians bedömning överensstämmelser i sak med regeringens.

Remissinstanserna: De remissinstanser som yttrar sig i frågan ställer sig bakom promemorians bedömning.

Skälen för regeringens bedömning

Sekretess i den brottsbekämpande verksamheten

Sekretesslagen (1980:100) ersattes den 30 juni 2009 av offentlighets- och sekretesslagen (2009:400; prop. 2008/09:150). Sekretess till skydd för intresset av att förebygga eller beivra brott regleras i 18 kap. offentlighets- och sekretesslagen (tidigare 5 kap. sekretesslagen). Sekretess gäller,

i större eller mindre utsträckning, för förundersökningar och motsvarande utredningar enligt 23 kap. rättegångsbalken (18 kap. 1 §) och som regel för underrättelseuppgifter (18 kap. 2 §). De sekretessbestämmelser till skydd för enskild som tidigare fanns i 9 kap. 17 § sekretesslagen har delats upp på flera paragrafer och finns nu huvudsakligen i 35 kap. offentlighets- och sekretesslagen, som reglerar sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott.

Sekretessen enligt 35 kap. 1 § offentlighets- och sekretesslagen (som motsvarar 9 kap. 17 § första stycket sekretesslagen) skyddar enskilds personliga och ekonomiska förhållanden. Sekretessen omfattar bl.a. uppgifter i utredning enligt bestämmelserna om förundersökning i brottmål (punkten 1), användning av tvångsmedel (punkten 2), registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (punkten 3), annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, en polismyndighet, Skatteverket, Statens kriminaltekniska laboratorium, Tullverket eller Kustbevakningen (punkten 4), register som förs av Rikspolisstyrelsen enligt polisdatalagen eller som annars behandlas där med stöd av den lagen (punkten 6) och misstankeregistret (punkten 7). Brottsanmälningar omfattas också av sekretessen. Sekretessen gäller endast om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående lider skada eller men. För beslut att väcka åtal eller att inte inleda eller lägga ned en förundersökning gäller inte sekretessen (35 kap. 6 §). Sekretessen upphör också normalt om uppgiften lämnas till domstol med anledning av åtal (35 kap. 7 §), men i en förundersökning förekommer det ofta uppgifter t.ex. om andra brott som den misstänkte har begått eller om personer som inte berörs av åtalet. För sådana uppgifter upphör sekretessen inte, om uppgiften uppenbart saknar betydelse i målet (35 kap. 7 § punkten 2). Om åtal inte väcks kvarstår också sekretessen. Därför är det mycket vanligt att det förekommer kvarstående sekretess till skydd för enskild i förundersökningar och andra brottsutredningar.

När en förundersökning eller annan motsvarande utredning inleds gäller som regel sekretess enligt både 18 kap. 1 eller 2 § och 35 kap. 1 § offentlighets- och sekretesslagen. Sekretessen enligt 18 kap. minskar efter hand och brukar normalt upphöra senast i samband med att åtal väcks.

Enligt 35 kap. 2 § gäller sekretess för uppgift i en anmälan eller utsaga av enskild i förhållande till den som anmälan eller utsagan avser, om det kan antas att fara uppkommer för att någon utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Bestämmelser om sekretess för vissa andra av polisens register än de som regleras i 35 kap. 1 § punkterna 6 och 7 finns i 35 kap. 3 och 4 §§. I 3 § regleras sekretessen för belastningsregistret (tidigare 7 kap. 17 § sekretesslagen). I 4 § (tidigare 7 kap. 18 § sekretesslagen) regleras sekretessen för bl.a. register över strafföreläggande och föreläggande av ordningsbot (punkten 1) och uppgift hos Rikspolisstyrelsen som rör brott eller den som har misstänkts, åtalats eller dömts för brott, om uppgiften har lämnats dit för databehandling inom rättsväsendets informationssystem i ett annat register än som avses i 1 § (punkten 2).

Några sekretessbrytande bestämmelser som tidigare fanns i 9 kap. 17 § finns nu i 35 kap. 8–10 §§. Dessa avser uppgiftslämnande till enskild och till konkursförvaltare och saknar därför intresse här.

Sekretess mellan brottsbekämpande myndigheter

Ansvaret för brottsbekämpningen i Sverige är uppdelat mellan flera myndigheter. Gemensamt för dessa är att sekretess i större eller mindre utsträckning gäller åtskilliga av de personuppgifter som behandlas inom ramen för den brottsbekämpande verksamheten. 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. Det är två kriterier som är viktiga vid bedömningen av om det är fråga om olika verksamhetsgrenar. Den ena är om verksamheterna tillämpar samma eller olika sekretessregler. Det andra är om verksamhetsgrenarna är åtskilda rent organisatoriskt (prop. 2008/09:150 s. 356 f.).

Offentlighets- och sekretesslagen innehåller bestämmelser som möjliggör utbyte av uppgifter mellan myndigheter utan hinder av sekretess. Av 10 kap. 2 § offentlighets- och sekretesslagen (tidigare 1 kap. 5 § 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 (tidigare 14 kap. 1 § sekretesslagen). Uppgifter kan vidare, 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 10 kap. 27 §, den s.k. generalklausulen (tidigare 14 kap. 3 § sekretesslagen), gäller som huvudregel att uppgifter får lämnas ut till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Undantag görs dock för vissa sekretessregler som är av begränsat intresse här. Bedömningen av om uppgiften kan lämnas ut görs av den myndighet som innehar uppgiften, utom i de fall där utlämnandebestämmelsen har konstruerats så att uppgiften alltid ska lämnas ut om det begärs.

Bestämmelsen i 6 kap. 5 § offentlighets- och sekretesslagen (tidigare 15 kap. 5 § sekretesslagen) är också viktig i sammanhanget. Den innebär att en myndighet på begäran av en annan myndighet ska lämna ut uppgifter i den mån hinder inte möter på grund av sekretess eller arbetets behöriga gång. Bestämmelsen kan sägas motsvara allmänhetens rätt att få tillgång till handlingar genom offentlighetsprincipen, men utlämnandeskyldigheten är mer vidsträckt och omfattar alla typer av uppgifter som

myndigheten förfogar över, bl.a. uppgifter i handlingar som inte är allmänna. Paragrafen innebär att om en myndighet begär att få del av uppgifter hos en annan myndighet och någon sekretessbrytande bestämmelse är tillämplig, så ska uppgifterna lämnas ut. Detsamma gäller givetvis om de begärda uppgifterna är offentliga.

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. polisdatalagen och i förordningar som meddelats med stöd av den lagen. Motsvarande bestämmelse infördes i sekretesslagen i samband med att den absoluta sekretessen för polisregister avskaffades (se prop. 1997/98:97) och har i sak oförändrad förts över till den nya offentlighets- och sekretesslagen. Syftet med bestämmelsen är bl.a. att myndigheterna inte ska behöva förlita sig på en sekretessprövning i de fall där det i författning anges att uppgifter får lämnas ut. I 6–8 §§ polisdatalagen (1998:622) finns bestämmelser om att uppgifter får lämnas ut. Sådana bestämmelser finns även i polisdataförordningen, se bl.a. 8, 10, 17, 17 a och 18 §§.

Beredningen för rättsväsendets utveckling har i betänkandet Ett effektivare brottmålsförfarande – några ytterligare åtgärder (SOU 2005:117 s. 152 f.) föreslagit att sekretessen i 9 kap. 17 § sekretesslagen (som numera regleras i olika paragrafer i framför allt 35 kap. offentlighets- och sekretesslagen) inte ska gälla vid informationsutbyte mellan brottsbekämpande myndigheter. Skälet är att den nuvarande regleringen inte täcker det behov som myndigheterna har av att utbyta information med varandra. Betänkandet, som har remissbehandlats, bereds i Regeringskansliet (Justitiedepartementet).

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 (se bl.a. prop. 2004/05:164 s. 83 och 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 (prop. 2007/08:160 s. 73). Direktåtkomst förutsätter därför att det är fråga om offentliga uppgifter, uppgifter som omfattas av en författningsbestämmelse om uppgiftsskyldighet eller – i undantagsfall – uppgifter som kan lämnas ut rutinmässigt med stöd av generalklausulen.

Den dåvarande regeringen gjorde i prop. 2004/05:164 Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling bedömningen att det krävs en tydlig sekretessbrytande reglering för att Tullverket utan risk för problem från sekretessynpunkt ska kunna medge andra brottsbekämpande myndigheter direktåtkomst, om direktåtkomsten ska avse annat än uppgifter som inte omfattas av sekretess. Därför infördes en sekretessbrytande bestämmelse i 2 § förordningen (2005:791) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Samma bedömning görs avseende Kustbevakningens möjlighet att lämna ut uppgifter i betänkandet Kustbevakningens personuppgiftsbehandling (SOU 2006:18) och avseende åklagarväsendet i betänkandet Åklagarväsendets brottsbekämpning – Integritet – Effektivitet (SOU 2008:87). Betänkandena har remissbehandlats och är föremål för beredning i Regeringskansliet (Försvarsdepartementet respektive Justitiedepartementet).

De skäl som anfördes i lagstiftningsärendet rörande Tullverkets personuppgiftsbehandling för att det behövs sekretessbrytande regler har bärkraft även när det gäller uppgiftslämnande från polisen. Flera remissinstanser har i sina yttranden över utredningens förslag påtalat behovet av sekretessbrytande regler även av andra skäl. Beredningen för rättsväsendets utveckling har övervägt det generella behovet av sekretessbrytande regler och kommit till samma slutsats. Det bör därför införas sekretessbrytande regler i den nya lagen.

Det har nyligen införts en särskild bestämmelse om överföring av sekretess vid direktåtkomst (prop. 2007/08:160). Om en myndighet hos en annan myndighet har elektronisk tillgång till en upptagning för automatiserad behandling och en uppgift i denna upptagning är sekretessreglerad blir sekretessbestämmelsen, enligt 11 kap. 4 § offentlighets- och sekretesslagen, tillämplig även hos den mottagande myndigheten. Sekretessen gäller dock inte om uppgiften ingår i ett beslut hos den mottagande myndigheten. Sekretessen enligt paragrafen ska inte heller tillämpas när det hos den mottagande myndigheten finns en annan primär sekretessbestämmelse än 21 kap. 1, 3, 5, och 7 §§ som skyddar samma intresse (11 kap. 8 § offentlighets- och sekretesslagen). Sekretessen enligt 11 kap. 4 § gäller för sådana uppgifter som andra myndigheter får tillgång till genom direktåtkomst till uppgifter som polisen behandlar. Eftersom samtliga brottsbekämpande myndigheter i princip tillämpar samma primära sekretessbestämmelser, och en bestämmelse om primär sekretess gäller framför den nu angivna paragrafen, får 11 kap. 4 § offentlighets- och sekretesslagen begränsad betydelse.

13.2 Sekretessgenombrott

Regeringens förslag: Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket samt 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen, rätt att ta del av uppgifter som har gjorts gemensamt tillgängliga hos polisen, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Under samma förutsättningar ska polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket ha rätt att ta del av uppgifter i fingeravtrycks- eller signalementsregister.

Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen har också, under samma förutsättningar, rätt att ta del av uppgifter om huruvida personer förekommer i register över DNA-profiler.

Bestämmelserna om sekretessgenombrott gäller även i förhållande till Säkerhetspolisen.

Statens kriminaltekniska laboratorium ska ha rätt att ta del av uppgifter i register över DNA-profiler samt fingeravtrycks- eller signalementsregister, om uppgifterna behövs i myndighetens verksamhet.

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

Utredningens förslag: Uppgifter som behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet och uppgifter ur det allmänna spaningsregistret ska få lämnas ut till övriga brottsbekämpande myndigheter, men endast om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder (se 3 och 4 §§ förslaget till förordning, SOU 2001:92, s. 209).

Remissinstanserna har inte haft någon invändning mot utredningens förslag.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår inte att sekretessen för uppgifter i register över DNA-profiler ska brytas i förhållande till Tullverket och Kustbevakningen.

Remissinstanserna: De remissinstanser som yttrar sig ställer sig i princip bakom förslaget. *Kammarrätten i Stockholm* anser dock att det av lagtexten bör framgå att andra brottsbekämpande myndigheter bara får tillgång till uppgifter när de behöver detta för att bedriva den brottsbekämpande verksamhet som de är ålagda enligt lag eller annan författning. *Tullverket* invänder mot förslaget att samla bestämmelserna om utlämnande av uppgifter i lagens andra kapitel. Verket tar också upp frågan om de sekretessbrytande bestämmelserna är uttömmande. *Rikspolisstyrelsen* anser att man i det fortsatta arbetet bör överväga om inte även vissa andra myndigheter, som deltar i samarbetet i regionala underrättelsecentrum, bör omfattas av sekretessgenombrott. *Åklagarmyndigheten* ifrågasätter

om man inte bör göra undantag också för sekretess i ärenden om besöksförbud.

Skälen för regeringens förslag

Sekretessgenombrott mellan de brottsbekämpande myndigheterna

För att öka möjligheterna till informationsutbyte med andra brottsbekämpande myndigheter (jfr avsnitt 12.1) och för att skapa förutsättningar för att polisen ska kunna medge direktåtkomst till uppgifter som gjorts gemensamt tillgängliga i dess brottsbekämpande verksamhet behövs det regler som bryter sekretess. Frågan är då hur dessa regler bör utformas.

Eftersom den sekretessbrytande bestämmelsen bl.a. ska möjliggöra direktåtkomst, måste sekretessprövningen göras innan direktåtkomsten beviljas. Sekretessprövningen kan därför inte vara alltför komplicerad. Den sekretessbrytande regeln måste således tillåta ett relativt brett sekretessgenombrott men i gengäld kommer den, som utvecklas närmare i det följande, att kompletteras med andra integritetsskyddande bestämmelser.

Enligt promemorian ligger det i sakens natur att en sekretessbrytande bestämmelse som ska möjliggöra direktåtkomst mellan brottsbekämpande myndigheter måste vara generellt utformad, eftersom det vid direktåtkomst saknas möjlighet att göra en sekretessprövning i varje enskilt fall. Prövningen måste i stället, som nämnts ovan, göras i förväg. Med hänsyn till intresset av ett gott skydd för den personliga integriteten anser promemorian att ett fullständigt sekretessgenombrott mellan de brottsbekämpande myndigheterna inte är acceptabelt. Även om sekretessen består gentemot allmänheten och effektivitetsaspekterna väger tungt, bör någon form av begränsning i den sekretessbrytande bestämmelsen göras. Uppgifter som omfattas av sekretess till skydd för enskild kan vara mycket integritetskänsliga. Därför är det viktigt att andra enheter inom polisen och andra brottsbekämpande myndigheter får tillgång till sådana uppgifter bara när de behöver det för att kunna bedriva den brottsbekämpande verksamhet som de är ålagda enligt lag eller annan författning. Enligt promemorian bör just detta behov utgöra det rekvisit som begränsar den sekretessbrytande bestämmelsen. Regeringen ställer sig bakom den bedömningen.

Då den föreslagna regeln har det uttryckliga syftet att tillåta frekvent utlämnande bör enligt regeringens mening behovsbedömningen kunna göras inom tämligen vida ramar. Bedömningen av vad mottagaren behöver får göras främst utifrån myndighetens brottsbekämpande uppgifter och med utgångspunkt i de behov som typiskt sett föreligger. Personuppgifter som en myndighet typiskt sett inte behöver bör alltså inte vara åtkomliga. Exempelvis får Skatteverkets brottsenheter typiskt sett anses ha behov av att få tillgång till uppgifter som rör ekonomisk brottslighet och andra brott som kan ha anknytning till sådan brottslighet (framför allt förmögenhetsbrott och vissa specialstraffrättsliga brott), medan dessa enheter mycket sällan torde ha behov av att ta del av uppgifter i t.ex. förundersökningar om brott mot person, brott mot allmänheten eller miljöbrott. När det gäller Tullverket kan myndigheten typiskt sett antas ha behov av bl.a. uppgifter om brott som rör varor som är förbjudna att föra

in eller ut ur landet, exempelvis narkotika, dopningsmedel och vissa typer av vapen. Detsamma gäller uppgifter om brott som rör ekonomisk brottslighet och andra brott med anknytning till sådana brott (jfr vad som sagts angående Skatteverkets behov). För Åklagarmyndighetens del kan en avgränsning inte bygga på brottstyper, eftersom åklagare har behov av uppgifter i alla typer av brottsutredningar. Där kan i stället t.ex. en begränsning avseende tillgången till vissa typer av uppgifter vara tänkbar. Man kan t.ex. göra skillnad mellan uppgifter om brottsutredningar och andra uppgifter. Ekobrottsmyndighetens behov får bedömas med utgångspunkt i myndighetens verksamhetsområde, som är betydligt smalare än Åklagarmyndighetens. Eftersom Ekobrottsmyndigheten sysselsätter både polismän och åklagare, måste å andra sidan beaktas myndighetens behov av tillgång till uppgifter som typiskt sett det särskilda samarbetet kräver. När Säkerhetspolisen för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet har Säkerhetspolisen ställning som polismyndighet och har likartade behov som övriga polismyndigheter av att få del av uppgifter. Säkerhetspolisen har även andra åligganden, bl.a. att fullgöra de uppgifter som åvilar Rikspolisstyrelsen enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Vilka personuppgifter som Säkerhetspolisen har behov av att kunna få del av för detta ändamål regleras i nämnda författningar med kompletterande föreskrifter. För att möjliggöra direktåtkomst bör således utgångspunkten för den sekretessbrytande regeln vara att den bör täcka de behov av information som andra brottsbekämpande myndigheter typiskt sett har.

Mot bakgrund av dessa överväganden bör den sekretessbrytande bestämmelsen utformas så att uppgifter i polisens brottsbekämpande verksamhet, trots viss närmare angiven sekretess, ska kunna lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen respektive Skatteverket under två förutsättningar. Den ena är att uppgifterna är gemensamt tillgängliga. Den andra är att den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Personuppgifter som inte är gemensamt tillgängliga omfattas således inte av bestämmelsen. Sådana uppgifter kan dock komma att lämnas ut efter en sekretessprövning i det enskilda fallet med stöd av andra bestämmelser.

Sekretessbrytande regler kan föreskrivas såväl i lag som förordning. Mot bakgrund av polisverksamhetens särskilda natur bör andra myndigheters tillgång till uppgifter som behandlas av polisen normalt regleras i lag. Sekretessbrytande bestämmelser bör därför tas in i den nya lagen.

Vilka sekretessbestämmelser ska den nya regleringen omfatta?

Frågan är då vilka slag av sekretess som ska kunna brytas. Eftersom bestämmelserna i 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen till skydd för intresset att förebygga och förhindra brott är tillämpliga hos alla brottsbekämpande myndigheter bör det i de flesta fall inte innebära någon skada för polisens verksamhet att lämna ut uppgifterna. Utgångspunkten är således redan enligt gällande rätt att uppgifter som omfattas av sekretess enligt nämnda paragrafer normalt kan lämnas ut till en annan

brottsbekämpande myndighet. Detta förutsätter emellertid att det är möjligt att på förhand bedöma om en viss förundersökning eller motsvarande kan lämnas ut. En sådan bedömning bör kunna göras för olika brottstyper eller olika slags underrättelseprojekt.

På motsvarande sätt bör det redan enligt gällande bestämmelser vara möjligt att bedöma den risk som kan vara förknippad med att lämna ut uppgifter som är sekretessbelagda med stöd av någon annan bestämmelse i 18 kap. offentlighets- och sekretesslagen.

Något generellt behov av att bryta den sekretess som kan gälla enligt 18 kap. 1 och 2 §§ kan således inte anses föreligga. I de fall där utlämnandet av en uppgift till en annan brottsbekämpande myndighet skulle innebära att polisens egen verksamhet riskerar att skadas, bör direktåtkomst givetvis inte komma ifråga. Det sagda gäller även övriga bestämmelser i 18 kap. I sådana fall får, som nyss nämnts, i stället övervägas om uppgiften kan lämnas ut med stöd av någon annan sekretessbrytande bestämmelse, exempelvis 10 kap. 2 eller 27 § offentlighets- och sekretesslagen.

Eftersom de flesta pågående eller avslutade förundersökningar som inte har lett till åtal och flertalet uppgifter i underrättelseverksamhet kringgärdas av sekretess enligt bestämmelser i 35 kap. offentlighets- och sekretesslagen till skydd för enskild, krävs det sekretessprövning i varje enskilt fall där en sådan uppgift ska lämnas till en annan brottsbekämpande myndighet. Även om uppgifterna kan lämnas ut efter en sådan prövning innebär det att tid och kraft måste läggas på en prövning som normalt alltid ger samma resultat. En sekretessbrytande regel skulle därför underlätta informationsutbytet.

Den paragraf i sekretesslagen som förslaget till sekretessbrytande regel i promemorian avser, 9 kap. 17 §, har delats upp på flera paragrafer i offentlighets- och sekretesslagen. Sekretessgenombrottet måste därför, för att få den avsedda effekten, omfatta fler bestämmelser, men kan i gengäld begränsas till de paragrafer som är relevanta för informationsutbyte mellan myndigheter.

Den sekretessbestämmelse som oftast torde vara tillämplig är 35 kap. 1 § offentlighets- och sekretesslagen, som reglerar sekretessen bl.a. i förundersökningar och andra liknande utredningar, i misstankeregistret och i flertalet andra register i den brottsbekämpande verksamheten. I tidigare utredningar har pekats på verksamhetsbehovet av att kunna bryta sekretessen enligt den bestämmelsen, eftersom det påtagligt skulle underlätta informationsutbytet mellan de brottsbekämpande myndigheterna. Sekretessen enligt 35 kap. 1 § är tillämplig hos alla brottsbekämpande myndigheter, vilket innebär att uppgifterna har samma skydd gentemot utomstående hos den mottagande myndigheten som hos den utlämnande myndigheten. Med hänsyn till de vinster för brottsbekämpningen som ett förenklat informationsutbyte skulle innebära kan enligt regeringens mening den ökade risken för integritetsintrång godtas. Motsvarande bedömning görs i fråga om sekretess för uppgifter i anmälan eller utsaga enligt 35 kap. 2 § offentlighets- och sekretesslagen.

Promemorian går igenom vissa andra sekretessbestämmelser i 7 och 9 kap. sekretesslagen som kan aktualiseras vid informationsöverföring mellan de brottsbekämpande myndigheterna. Dessa bestämmelser finns

numera i huvudsak i 35 kap. offentlighets- och sekretesslagen. Promemorian överväger bl.a. behovet av genombrott för sekretess

– för kopplingen mellan fingerade och verkliga personuppgifter,

– för säkerhetsarbetet för att skydda bl.a. hotade vittnen,

– för uppgift som rör utlänning och verksamhet som rör kontroll över utlänningar,

– i ärenden om besöksförbud och

– för uppgifter om enskilda i vissa framställningar i Schengensamarbetet.

Enligt promemorian finns det inte anledning att låta sekretessgenombrottet omfatta fler bestämmelser. Regeringen delar den uppfattningen. Sekretessgenombrottet bör därför inte omfatta någon av de andra paragraferna i 35 kap.

Av sekretessreglerna i 35 kap. offentlighets- och sekretesslagen bör alltså den sekretessbrytande regeln endast omfatta sekretess enligt 1 och 2 §§. I den mån andra sekretessbestämmelser i kapitlet är tillämpliga får det, på samma sätt som nu, göras en bedömning i det enskilda fallet av huruvida sekretessen hindrar att uppgifterna lämnas ut till en annan brottsbekämpande myndighet.

Sekretessen i 21 kap. 3 § första stycket offentlighets- och sekretesslagen (tidigare 7 kap. 1 a § sekretesslagen) gäller för uppgift om enskilds bostadsadress, telefonnummer och andra jämförbara uppgifter som kan användas för att komma i kontakt med den enskilde, om det finns särskild anledning att anta att han eller hon, eller någon närstående, kan komma att utsättas för våld eller annat allvarligt men om uppgiften röjs. Denna sekretess har införts för att säkerställa skyddet för det som brukar kallas skyddade adresser hos alla myndigheter (se prop. 2005/06:161 s. 55 f.).

Sekretessen i paragrafens första stycke skyddar personer som anses ha stort behov av att uppgifter om deras uppehållsort inte röjs. Sekretess enligt denna paragraf är relativt vanlig i brottsutredningar. Ibland gäller sekretessen till skydd för brottsoffret och ibland till skydd för den misstänkte. Sekretess enligt 21 kap. 3 § första stycket offentlighets- och sekretesslagen gäller hos alla myndigheter. Det innebär att en uppgift som lämnas till en annan brottsbekämpande myndighet har samma skydd gentemot allmänheten hos den mottagande myndigheten. Dessutom är de brottsbekämpande myndigheterna vana vid att hantera denna sekretess. Mot den nu angivna bakgrunden bör uppgifter som omfattas av sekretess enligt 21 kap. 3 § första stycket kunna lämnas vidare utan hinder av sekretessen.

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 får utlämnande bara avse uppgifter som har gjorts gemensamt tillgängliga. Detta innebär i sig en begränsning, eftersom en del av de uppgifter som polisen behandlar aldrig kommer att göras gemensamt tillgängliga. För behandlingen av gemensamt tillgängliga uppgifter ska (som framgår av bl.a. avsnitt 9 och 11) gälla särskilda begränsningar, vilket bl.a. innebär att enligt huvudregeln bara vissa typer av uppgifter ska vara åtkomliga vid sökning. Vidare ska det framgå för vilket ändamål uppgiften behandlas. Upplysningar som rör misstänkt brottslig verk-

samhet ska förses med upplysning om källans tillförlitlighet och uppgifternas riktighet i sak. 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 registerförfattningar – som i likhet med polisens 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 på personuppgifter ska begränsas till vad den enskilde tjänstemannen behöver för att fullgöra sina arbetsuppgifter. Alla regler om sekretess som kan vara tillämpliga i polisens verksamhet kommer inte heller att genombrytas. Sammantaget innebär förslaget att den sekretessbrytande regeln skapar förutsättningar för bättre informationsutbyte i brottsbekämpningen, samtidigt som risken för integritetsintrång beaktas.

Åklagarmyndigheten ifrågasätter om inte även sekretessen i ärenden om besöksförbud (35 kap. 5 § offentlighets- och sekretesslagen) bör omfattas av sekretessgenombrottet. I promemorian avvisas detta under hänvisning till att uppgifter i sådana ärenden sällan är av generellt intresse för andra brottsbekämpande myndigheter. Utredningar om besöksförbud tar framför allt sikte på brott mot personers liv, hälsa, frihet eller frid. Brotten riktar sig oftast mot nära anhöriga eller personer med vilka gärningsmannen har eller tidigare har haft någon form av relation. Polis och åklagare är de enda som utreder brott av detta slag. De uppgifter som förekommer i sådana ärenden rör ofta känsliga frågor i personernas privatliv och har som regel inte samma allmänna intresse som uppgifter om andra typer av brott. Mot den bakgrunden finns det enligt regeringens mening inte skäl att utvidga sekretessgenombrottet utöver vad som föreslås i promemorian.

Tullverket tar upp frågan hur den i promemorian föreslagna generella sekretessbrytande regeln förhåller sig till generalklausulen i 14 kap. 3 § sekretesslagen (numera 10 kap. 27 § offentlighets- och sekretesslagen). Bestämmelserna om sekretessgenombrott i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet reglerar inte uttömmande möjligheterna att lämna ut uppgifter mellan brottsbekämpande myndigheter. De syftar enbart till att underlätta frekvent uppgiftslämnande mellan dessa genom att inte ställa krav på sekretessprövning i det enskilda fallet för sådan sekretess och under de förutsättningar som anges i bestämmelserna. Det bör genom en hänvisning i lagen framgå att det finns bestämmelser om utlämnande även i offentlighets- och sekretesslagen.

Sammanfattningsvis bör således personuppgifter som har gjorts gemensamt tillgängliga kunna lämnas till en annan brottsbekämpande myndighet utan hinder av sekretess enligt 21 kap. 3 § första stycket samt 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen, om den mottagande myndigheten har behov av uppgiften i sin brottsbekämpande verksamhet. I den mån andra sekretessbestämmelser är tillämpliga får det, på samma sätt som nu, göras en bedömning i det enskilda fallet av huruvida sekretessen hindrar att uppgifterna lämnas ut till en annan brottsbekämpande myndighet.

Särskilt om vissa register

DNA-register, fingeravtrycks- och signalementsregister särregleras i polisdatalagen. I avsnitt 15 redovisas skälen för en fortsatt särreglering av sådana register. Där utvecklas att utgångspunkten bör vara att registren och deras användning i allt väsentligt regleras på samma sätt som nu. Vissa myndigheter har redan direktåtkomst till uppgifter i registren. Det aktualiserar frågan om man bör införa regler om sekretessgenombrott för uppgifter i register av detta slag. En regel om sekretessgenombrott underlättar för den registeransvariga myndigheten när den ska ta ställning till om en annan brottsbekämpande myndighet kan medges direktåtkomst till registren. Detta talar för att man bör införa regler om sekretessgenombrott även för uppgifter i dessa register.

Det finns för närvarande inte någon möjlighet att bevilja direktåtkomst till penningtvättsregister. Detsamma gäller motsvarigheten till det internationella registret. Någon direktåtkomst föreslås inte heller, bl.a. av det skälet att registren innehåller känsliga uppgifter. Det finns därför inte något skäl att införa bestämmelser om sekretessgenombrott för uppgifter i dessa register. Uppgifter kan dock lämnas ut efter sedvanlig sekretessprövning.

Uppgiftsskyldighet till statistikmyndighet

I 6 § polisdatalagen föreskrivs att uppgifter som är nödvändiga för att framställa rättstatistiken ska lämnas till den myndighet som ansvarar för att framställa sådan statistik. Enligt förordningen (2001:100) om den officiella statistiken är det Brottsförebyggande rådet som är statistikansvarig myndighet. En bestämmelse om att uppgifter ska lämnas ut för statistikändamål bör finnas även i den nya lagen. Det kan anmärkas att enligt 24 kap. 8 § första stycket offentlighets- och sekretesslagen gäller absolut sekretess för personuppgifter i verksamheten hos myndighet som framställer statistik.

Den lagtekniska utformningen

Kammarrätten i Stockholm anser att det bör framgå av lagtexten att uppgifterna behövs i sådan brottsbekämpande verksamhet som myndigheten är ålagd enligt lag eller annan författning. Polisen och Åklagarmyndigheten har till uppgift att bekämpa alla typer av brott. Både Tullverket och Kustbevakningen har visserligen ett begränsat mandat att bedriva brottsbekämpning, men gränserna för detta är inte helt tydliga. Detsamma gäller Ekobrottsmyndigheten. Däremot har Skatteverket i lag tydligt avgränsade brottsbekämpande uppgifter. Mot den bakgrunden skulle den av kammarrätten föreslagna formuleringen inte fylla någon funktion för att begränsa tillämpningsområdet men skulle däremot kunna skapa osäkerhet angående tillämpningen. Det får vidare anses ligga i sakens natur att den verksamhet som respektive myndighet bedriver utförs i enlighet med det regelverk som gäller.

Tullverket kritiserar att de sekretessbrytande bestämmelserna har samlats i lagens andra kapitel. Verket förordar att regeln om sekretessge-

nombrott för gemensamt tillgängliga uppgifter placeras i tredje kapitlet och reglerna om sekretessgenombrott för uppgifter i register över DNA-profiler och fingeravtrycksregister i fjärde kapitlet, eftersom det skulle underlätta för tillämparen. Det finns enligt regeringens mening både för- och nackdelar med den lösning som har föreslagits i promemorian. Vissa av de föreslagna sekretessbrytande reglerna är tillämpliga på all personuppgiftsbehandling i polisens brottsbekämpande verksamhet och har därmed sin naturliga plats i andra kapitlet, medan några av reglerna har ett smalare tillämpningsområde. Ett viktigt skäl till att hålla samman de sekretessbrytande reglerna är att kunna ge tillämparen en samlad bild av vilka bestämmelser som bryter sekretess. En uppdelning av de sekretessbrytande bestämmelserna mellan olika kapitel förutsätter att vissa bestämmelser upprepas på flera ställen och att hänvisningar görs mellan paragraferna. Att placera bestämmelserna om sekretessgenombrott i register med DNA-profiler och fingeravtrycksregister tillsammans med reglerna om dessa register kan ge intrycket av att det är en uttömmande reglering. Så är emellertid inte fallet, eftersom regeln om utlämnande av uppgifter till utländsk myndighet är generell och även omfattar uppgifter ur register med DNA-profiler och fingeravtrycksregister i enlighet med våra internationella åtaganden. Fördelarna med en samlad reglering av de sekretessbrytande bestämmelserna väger därför över.

Det bör tydliggöras i lagen att regeringen på samma sätt som nu har möjlighet att meddela föreskrifter om att uppgifter får lämnas ut även i andra fall än de som har redovisats ovan.

13.3 Uppgiftslämnande till utlandet

Regeringens förslag: Om det är förenligt med svenska intressen får personuppgifter lämnas till

1. en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott, eller
2. en utländsk underrättelse- eller säkerhetstjänst.

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

Utredningens förslag överensstämmer i sak med promemorians.

Remissinstanserna har antingen ställt sig bakom eller inte kommenterat förslaget.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna kommenterar i allmänhet inte förslaget. *Kustbevakningen* är positiv till förslaget. *Statens kriminaltekniska laboratorium* understryker att lagstiftningen måste leva upp till de krav som Prümsamarbetet ställer.

Skälen för regeringens förslag

Nuvarande möjligheter att lämna ut uppgifter

En utgångspunkt i offentlighets- och sekretesslagen är att en uppgift som omfattas av sekretess inte får röjas för en utländsk myndighet. Enligt 8 kap. 3 § offentlighets- och sekretesslagen får en sekretesskyddad uppgift röjas för en utländsk myndighet eller en mellanfolklig organisation i två situationer. Den ena är när utlämnandet sker enligt särskild föreskrift i lag eller författning. Den andra är när uppgiften i motsvarande fall skulle få lämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas.

I 10 kap. 2 § offentlighets- och sekretesslagen föreskrivs att sekretess inte hindrar att en uppgift lämnas ut om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin egen verksamhet. Enligt förarbetena är denna sekretessbrytande bestämmelse avsedd att tillämpas restriktivt. Inom vissa myndighetsområden, som exempelvis polisens brottsbekämpande verksamhet, är det i ganska stor utsträckning nödvändigt att lämna ut sekretessbelagda uppgifter med stöd av den bestämmelsen. Ett typiskt exempel i det internationella samarbetet är att en svensk myndighet i samband med begäran om rättslig hjälp i en förundersökning lämnar uppgifter som omfattas av sekretess enligt 18 kap. 1 eller 2 § och 35 kap. 1 § offentlighets- och sekretesslagen till en utländsk åklagar- eller polismyndighet i syfte att få ett visst förhör genomfört. Om det är nödvändigt för en myndighet att lämna ut sekretessbelagda uppgifter för att myndigheten ska kunna fullgöra sin egen verksamhet står det i regel klart att det är förenligt med svenska intressen att lämna uppgifterna. I det följande diskuteras inte sådant internationellt samarbete som sker i svenskt intresse, utan uteslutande samarbete i syfte att bistå andra länder i deras brottsbekämpande verksamhet.

Enligt 18 kap. 18 § offentlighets- och sekretesslagen får, utan hinder av bestämmelsen i 17 § samma lag om sekretess till skydd för rättsligt samarbete på begäran av annan stat eller mellanfolklig organisation, uppgifter lämnas ut om detta har stöd i en bestämmelse i polisdatalagen eller i lagen om Schengens informationssystem.

Enligt 7 § polisdatalagen (1998:622) får uppgifter lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Regeringen får meddela föreskrifter om visst sådant uppgiftslämnande. I 18 § polisdataförordningen (1999:81) föreskrivs att uppgifter som behandlas enligt polisdatalagen får lämnas ut i två olika situationer, om det är förenligt med svenska intressen. Den ena är utlämnande till utländsk underrättelse- eller säkerhetstjänst. Den andra är utlämnande till en utländsk polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. Bestämmelserna är sekretessbrytande. Reglerna i 7 § polisdatalagen och 18 § polisdataförordningen dispenserar emellertid inte från bestämmelserna i personuppgiftslagen om överföring av personuppgifter till tredjeland. Vid utlämnande av personuppgifter till utlandet måste polisen där-

för också göra en bedömning av om reglerna i personuppgiftslagen hindrar utlämnande.

Utgångspunkterna för den nya regleringen

Det är framför allt i tre olika situationer som informationsutbyte aktualiseras i internationellt polisiärt samarbete. Den första är där Sverige i en bindande internationell överenskommelse har förbundit sig att tillhandahålla information av visst slag utan särskild anmodan, genom direktåtkomst eller på annat sätt. Den andra är där Sverige i en sådan överenskommelse har åtagit sig att genomföra en viss åtgärd eller att lämna viss information på begäran av en annan stat eller mellanfolklig organisation. Den tredje situationen är s.k. spontant uppgiftsutlämnande, där initiativet till informationsutbytet tas av den svenska polisen. Sådant informationsutbyte kan bygga på en internationell överenskommelse, men behöver inte göra det.

Promemorian har som utgångspunkt att uppgifter ska kunna lämnas till en utländsk myndighet eller mellanfolklig organisation i samma utsträckning som enligt gällande reglering. Enligt promemorian förutsätter ett väl fungerande samarbete över gränserna att den svenska polisen inte bara bistår polismyndigheter i andra länder med svar på konkreta förfrågningar eller med rättslig hjälp i enskilda ärenden utan även att svensk polis kan lämna uppgifter spontant i de fall där utbytet främst gagnar utländska intressen. Som framhålls i promemorian är möjligheten att bryta sekretess med stöd av 8 kap. 3 § offentlighets- och sekretesslagen inte tillräcklig för att Sverige ska kunna fullgöra sina internationella åtaganden utan det behövs särskilda sekretessbrytande bestämmelser.

Eftersom ett av syftena med den nya lagen är att åstadkomma en tydligare reglering av förutsättningarna för uppgiftslämnandet mellan svenska brottsbekämpande myndigheter är det, som framhålls i promemorian, naturligt att också uppgiftslämnande till utländska brottsbekämpande myndigheter och organisationer i huvudsak regleras i lagen. Lagen bör därför innehålla de grundläggande reglerna om uppgiftslämnande, medan kompletterande regler liksom nu kan finnas i förordning.

Bindande åtaganden om att lämna uppgifter

Den nya lagens bestämmelse om utlämnande av uppgifter till utländska myndigheter och mellanfolkliga organisationer bör omfatta folkrättsligt bindande åtaganden om att lämna viss information till en annan stat eller till en mellanfolklig organisation. I promemorian diskuteras huruvida denna bestämmelse ska möjliggöra utlämnande av uppgifter oberoende vem som har ingått de internationella överenskommelserna, mot bakgrund av att Rikspolisstyrelsen, efter bemyndigande från regeringen, har ingått bilaterala avtal om polisiärt samarbete med vissa stater. Regeln om uppgiftslämnande till en utländsk myndighet eller mellanfolklig organisation bör i likhet med gällande lagstiftning och i enlighet med vad som föreslås i promemorian endast omfatta internationella åtaganden som har godkänts av riksdagen.

Informationsutbyte med polis- och åklagarmyndigheter m.m. på begäran

Det förhållandet att uppgiftslämnande till utländska polis- och åklagarmyndigheter sker frekvent talar enligt promemorian för att man bör reglera detta direkt i lagen, i stället för att som nu ha ett bemyndigande för regeringen att meddela föreskrifter om utlämnande. Regeringen delar bedömningen att den sekretessbrytande regeln för informationsutbyte på begäran av utländska polis- och åklagarmyndigheter bör finnas i lag. Förutsättningen för att lämna uppgifter till utländska brottsbekämpande myndigheter eller organisationer bör vara att uppgiften behövs för att förebygga, förhindra, upptäcka, utreda eller beivra brott. Dessutom ska utlämnandet vara förenligt med svenska intressen.

Sverige har förbundit sig att på begäran lämna vissa uppgifter till andra stater som är anslutna till Europol. Det följer således redan av den föreslagna regeln om folkrättsligt bindande åtaganden att information kan lämnas på begäran av en sådan stat, men en tydlig reglering av vilken det framgår att uppgifter alltid får lämnas till stater som tillhör Europol, om förutsättningarna i övrigt är uppfyllda, underlättar för tillämparen. Regleringen bör också omfatta uppgiftslämnandet till själva organisationen.

Sverige har även förbundit sig att inom ramen för Interpol lämna andra stater bistånd med information, men dessa åtaganden är inte lika långtgående som när det gäller åtagandena i förhållande till stater som är medlemmar i Europol. Likaså har Sverige förbundit sig att lämna viss information till Interpol i dess egenskap av samarbetsorganisation. Den nya lagen bör därför ge utrymme för att uppgifter kan lämnas både till en annan stat som är medlem i Interpol och till organisationen som sådan.

Bestämmelsen bör utformas så att det direkt framgår att personuppgifter får lämnas till polis- och åklagarmyndigheter i stater som är anslutna till Interpol. Därmed täcks även motsvarande uppgiftslämnande till stater som ingår i Europol, eftersom staterna inom EU är medlemmar i båda. Vidare bör utlämnande få ske till båda organisationerna.

Frågor om Prümsamarbetet behandlas närmare i avsnitt 15.

Spontant uppgiftslämnande

Ett flertal konventioner och andra internationella överenskommelser som rör brottsbekämpning och som Sverige har undertecknat, innehåller bestämmelser om spontant uppgiftslämnande. I den mån sådana bestämmelser hänvisar till nationell rätt betraktas de inte som obligatoriska förpliktelser. I promemorian lämnas ett flertal exempel på sådana åtaganden (Ds 2007:43 s. 250). Det finns emellertid även överenskommelser som ålägger svenska myndigheter en uttrycklig skyldighet att, utan föregående begäran, informera en annan stat om uppgifter som den kan ha nytta av i sin brottsbekämpning. I de fallen förutsätts den svenska myndigheten, om den har tillgång till information som bedöms ha betydelse för den andra statens brottsbekämpning, självmant kontakta sin motsvarighet i en annan stat. Prümrådsbeslutet innehåller sådana bestämmelser.

Den nya lagen måste ge utrymme för att den svenska polisen spontant lämnar ut information till en annan stats brottsbekämpande myndighet, om informationen är värdefull för den statens brottsbekämpning. Som exempel kan nämnas information om nya tillvägagångssätt vid allvarlig

gränsöverskridande brottslighet eller upplysningar om konkreta brott. Om uppgifter lämnas spontant kan informationen som regel förses med villkor att den mottagande staten bara får använda den på visst sätt eller för visst ändamål. Ett sådant villkor, som är bindande för mottagaren, kan underlätta informationsutbytet i enskilda fall. Ett villkor angående användningen kan bl.a. skydda mot att uppgifterna sprids vidare och utgör därför ett integritetsskydd för den enskilde.

Uppgifter bör alltså även i fortsättningen kunna lämnas till en utländsk polis- eller åklagarmyndighet, eller till Interpol eller Europol, utan föregående begäran. Det enda krav som bör ställas i den nya lagen, utöver att uppgifterna ska behövas i mottagarens brottsbekämpning, är att uppgiftslämnandet ska vara förenligt med svenska intressen.

Utlämnande till utländsk underrättelse- eller säkerhetstjänst

Internationellt informations- och erfarenhetsutbyte utgör en viktig del av Säkerhetspolisens verksamhet. Den brottslighet som Säkerhetspolisen har till uppgift att förebygga och avslöja är nämligen i många fall gränsöverskridande till sin natur. Terrorism bedrivs t.ex. ofta av terrornätverk med omfattande internationella förgreningar. Spionerioch andra brott mot rikets säkerhet har av naturliga skäl normalt utländska kopplingar. Eftersom utbyte av underrättelseinformation är en viktig förutsättning för Säkerhetspolisens arbete, bör uppgifter i samma utsträckning som nu kunna lämnas till en utländsk underrättelse- eller säkerhetstjänst, om det är förenligt med svenska intressen. Bestämmelsen om detta bör tas in i den nya lagen i stället för i förordning, eftersom det är fråga om frekvent uppgiftslämnande. Någon annan begränsning än att utlämnandet ska vara förenligt med svenska intressen bör inte uppställas för dessa fall.

Utlämnande i andra fall

Uppgifter kan även lämnas till en utländsk myndighet eller mellanfolklig organisation efter en sekretessprövning enligt 8 kap. 3 § offentlighets- och sekretesslagen. Det kan t.ex. vara fråga om uppgiftslämnande till någon annan mottagare än de som anges i lagen eller utlämnande för något annat ändamål.

Det bör tydliggöras i lagen att regeringen har möjlighet att meddela sekretessbrytande föreskrifter om utlämnande av uppgifter för andra ändamål eller till andra utländska mottagare än de som angetts i det föregående.

Överföring av uppgifter till tredjeland

Vid utlämnande av personuppgifter till utlandet måste polisen också göra en bedömning av om reglerna i personuppgiftslagen hindrar utlämnande. Enligt 33 § personuppgiftslagen (1998:204) är det förbjudet att föra över personuppgifter till tredjeland, dvs. ett land utanför Europeiska unionen och EES-området, om landet inte har en adekvat nivå för skydd av personuppgifter. Trots förbudet i 33 § är det enligt 34 § tillåtet att under vissa förutsättningar föra över uppgifter till tredjeland, bl.a. om den regi-

strerade ger sitt samtycke till överföringen. I avsnitt 6.4.2 förslås att reglerna i personuppgiftslagen om överföring av uppgifter till tredjeland även fortsättningsvis ska tillämpas på polisens personuppgiftsbehandling i den brottsbekämpande verksamheten.

De stater som tillhör Europol har samtliga tillträtt dataskyddskonventionen, vilket innebär att reglerna i 33 § personuppgiftslagen inte hindrar överföring av personuppgifter (34 § andra stycket personuppgiftslagen). Motsvarande gäller organisationen Europol.

När det gäller stater som enbart är anslutna till Interpol har vissa av dessa också tillträtt dataskyddskonventionen och har således en dataskyddsnivå som medger överföring av personuppgifter utan någon särskild bedömning. Även många andra stater har i och för sig en tillräcklig dataskyddsnivå, men det kräver en bedömning i det enskilda fallet. Interpol som organisation anses också uppfylla kraven på tillräcklig dataskyddsnivå.

Uppgiftslämnande till en polis- eller åklagarmyndighet i en annan stat som enbart är medlem i Interpol förutsätter alltså en noggrannare bedömning, eftersom den utlämnande myndigheten då – utöver att bedöma om det ligger i svenskt intresse att lämna uppgiften – alltid måste avgöra om den andra staten har en tillräcklig dataskyddsnivå för att överföring av personuppgifter ska vara tillåten enligt personuppgiftslagen.

14 Bevarande och gallring

14.1 Allmänt om bevarande och gallring

Regeringens förslag: Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de i lagen angivna ändamålen. Denna generella bestämmelse om längsta tid för bevarande ska kompletteras med bestämmelser som anger tidpunkter för när uppgifter senast måste gallras eller inte längre får behandlas i den brottsbekämpande verksamheten.

Regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att uppgifter – trots bestämmelser om gallring – får bevaras för historiska, statistiska eller vetenskapliga ändamål. Vidare kan regeringen, för vissa kategorier av uppgifter, meddela föreskrifter om att uppgifter får bevaras under längre tid än vad som anges i lagen.

Regeringens bedömning: Personuppgifter som inte längre får behandlas för brottsbekämpande ändamål och som bevaras automatiserat för arkivändamål bör avskiljas.

Utredningens förslag överensstämmer delvis med promemorians. I de fall där inga särskilda gallringsregler gäller ska enligt utredningen gallring ske om personuppgifterna inte längre behövs för ändamålet med behandlingen. Personuppgifter får dock bevaras längre för historiska, statistiska och vetenskapliga ändamål. Bestämmelserna om gallring föreslås inte vara tillämpliga på uppgifter i förundersökningar.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

Promemorians förslag överensstämmer i huvudsak med regeringens förslag och bedömning. Promemorian har dock inte föreslagit någon uttrycklig bestämmelse om att uppgifter aldrig får bevaras längre än vad som behövs för något eller några av lagens ändamål.

Remissinstanserna: Flertalet av remissinstanserna ställer sig bakom promemorians förslag eller har inget att invända mot det. Majoriteten av remissinstanserna yttrar sig dock inte särskilt angående bevarande och gallring. Några remissinstanser, däribland *Åklagarmyndigheten, Ekobrottsmyndigheten* och *Rikspolisstyrelsen*, anser att bestämmelserna är komplicerade och svårtillgängliga och efterlyser förenklingar. Enligt Rikspolisstyrelsen kommer det att vara både praktiskt och tekniskt svårt att tillämpa den föreslagna mängden gallringsregler. Styrelsen anser vidare att gallringsbestämmelserna i vissa fall är för snävt tilltagna. Styrelsen framhåller samtidigt att polisen har ett eget intresse av att gallra sådan information som inte längre behövs, eftersom överskott av information ger svårigheter att hitta ”rätt” information och är belastande för informations- och analysarbetet.

Rikspolisstyrelsen förklarar att styrelsen gör bedömningen att utgallrade uppgifter torde kunna föras över till ett digitalt arkiv och där behandlas för de ändamål som anges i arkivlagen (1990:782) samt gallras enligt bestämmelserna där. Styrelsen, liksom *Datainspektionen* och *Kustbevakningen*, anser att frågan om förutsättningarna för digital arkivering av uppgifter och vad som ska gälla för behandlingen av sådana uppgifter bör klargöras i den fortsatta beredningen.

Datainspektionen anser att den föreslagna regleringen av bevarande och gallring inte uppfyller kraven i artikel 5 e i dataskyddskonventionen. Enligt inspektionens bedömning krävs enligt konventionen antingen ett generellt lagstadgande av innebörd att uppgifter ska gallras när de inte längre behövs för det ändamål för vilket de samlades in eller att en behovsprövning görs på förhand genom meddelande av mer preciserade gallringsbestämmelser. Datainspektionen anser inte att de föreslagna gallringsbestämmelserna eller bestämmelserna om längsta tid för bevarande i den brottsbekämpande verksamheten är tillräckligt preciserade. Bestämmelserna medför enligt Datainspektionen att samma fasta tider ska tillämpas beträffande situationer i vilka polisen måste anses ha vitt skilda behov av att bevara uppgifterna. Inspektionen hänvisar bl.a. till artikel 7:1 andra stycket i Europarådets rekommendation No. R (87) 15 om användning av personuppgifter inom polissektorn, där det anges att behovet av bevarande av personuppgifter bör övervägas utifrån olika kriterier, bl.a. behovet av att bevara uppgifter i ljuset av utgången i ett ärende; ett slutligt domstolsutslag; särskilt ett frikännande; upprättelse; avtjänat straff; benådning; den registrerades ålder och skilda kategorier av data. Sammantaget anser Datainspektionen att den föreslagna regleringen inte bör ligga till grund för lagstiftning.

Riksarkivet godtar inte promemorians antagande att det ligger i den registrerades intresse att personuppgifter gallras. Integritetskänsliga uppgifter bör i stället skyddas och integritetsintrång motverkas genom bestämmelser om sekretess och om att uppgifterna inte görs tillgängliga. Enligt Riksarkivet bör arkivlagens regler gälla så att gallring kan ske när

uppgifterna inte behövs i verksamheten och behovet av insyn avtagit. Det möjliggör för Riksarkivet att i samarbete med myndigheten föreskriva om gallring och säkerställa en rationell arkivhantering och bevarande av uppgifter för historiska, statistiska eller vetenskapliga ändamål. Enligt Riksarkivet går den föreslagna lagstiftningen bara delvis på den av myndigheten förordade linjen. Riksarkivet framhåller att det är viktigt att regeringen utnyttjar möjligheten att bemyndiga Riksarkivet att meddela föreskrifter om att uppgifter, som enligt lagen ska gallras, får bevaras för arkivändamål.

Skälen för regeringens förslag och bedömning

Allmänt om bevarande och gallring

När stora mängder uppgifter om enskilda personer samlas hos myndigheter uppstår oundvikligen integritetsrisker, i synnerhet som dagens teknik tillåter att avancerade sammanställningar av information görs på ett enkelt sätt. En metod att minska integritetskänsligheten är att se till att uppgifter som inte längre behövs för en myndighets verksamhet avlägsnas från myndighetens databaser eller register. För att uppnå detta krävs bestämmelser om gallring av uppgifter eller bestämmelser som föreskriver begränsningar i möjligheten att behandla uppgifterna i myndighetens verksamhet.

Med gallring avses att handlingar eller uppgifter sorteras ut och förstörs. När det gäller gallring av elektroniska upptagningar innebär detta normalt att viss information raderas från databäraren, dvs. det fysiska underlaget. Den egentliga informationen som finns på ett elektroniskt medium behöver dock inte förstöras för att det ska vara fråga om gallring i traditionell mening. Material kan gallras genom att den elektroniskt lagrade informationen överförs till en pappersutskrift, varefter den raderas från det elektroniska mediet.

Vid utformningen av gallringsbestämmelser måste det beaktas att vissa uppgifter behöver bevaras för framtiden för att offentlighetsprincipen inte ska bli verkningslös. Uppgifter får i princip aldrig gallras i sådan omfattning att det äventyrar arkivens roll som en del av kulturarvet eller något av de tre huvudändamålen med arkivverksamheten. Även efter en genomförd gallring måste arkiven kunna tillgodose rätten att ta del av allmänna handlingar, rättsskipningens och förvaltningens behov samt forskningsbehov. Det går alltså inte att undantagslöst föreskriva att samtliga uppgifter ska gallras när de inte längre behövs för verksamheten. Tvärtom behövs en avvägning mellan integritets- och offentlighetsintresset. Detta är viktigt inte minst i en tid då mängder av uppgifter endast finns i elektronisk form. Att utplåna samtliga uppgifter i ett dataregister eller ett ärendehanteringssystem kan omöjliggöra en senare rekonstruktion av ett händelseförlopp.

Sedan år 2003 föreskrivs i 2 kap. 18 § tryckfrihetsförordningen att grundläggande bestämmelser om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande av sådana handlingar ska meddelas i lag. Bestämmelser om bevarande och gallring finns framförallt i arkivlagen (1990:782) men även i författningar som reglerar behandling av personuppgifter.

Handlingsoffentligheten bärs upp av arkivsystemet som innebär att allmänna handlingar ska bevaras i arkiv. Enligt 3 § arkivlagen ska myndigheters arkiv bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättsskipningen och förvaltningen samt forskningens behov. Allmänna handlingar får enligt 10 § samma lag gallras, men vid gallringen ska det beaktas att det arkivmaterial som återstår ska kunna tillgodose de ändamål som anges i 3 §. Enligt 14 § arkivförordningen (1991:446) får statliga myndigheter gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet, eller enligt särskilda gallringsföreskrifter i lag eller förordning. Arkivlagens utgångspunkt är att allmänna handlingar ska bevaras. Syftet med arkivering är att spegla verksamheten som den såg ut. Helst ska inget förändras. Att uppgifter arkiverats hindrar inte att uppgifterna på samma sätt som tidigare är sökbara och tillgängliga i verksamheten.

Gallring enligt Riksarkivets föreskrifter görs för att begränsa arkivens omfattning och för att arkiven inte ska tyngas av handlingar som saknar påtagligt informationsvärde, dvs. gallring görs av både ekonomiska skäl och hanteringsskäl.

Gallring görs även för att skydda den enskildes integritet. Sådana föreskrifter finns vanligtvis i de författningar som reglerar myndigheters personuppgiftsbehandling, s.k. registerförfattningar.

Som gallring räknas enligt Riksarkivets föreskrifter förstöring av allmänna handlingar och uppgifter i allmänna handlingar (se t.ex. 2 kap. 1 § RA–FS 2003:3). All överföring av uppgifter som medför informationsförluster för användaren betraktas därmed också som gallring. Överföring till annan databärare räknas enligt Riksarkivet som gallring om överföringen medför:

– informationsförlust,
– förlust av sökmöjligheter, eller
– förlust av möjlighet att fastställa informationens autenticitet.

Offentlighets- och sekretesskommittén gav i betänkandet Ordning och reda bland allmänna handlingar (SOU 2002:97 s. 73) en liknande beskrivning av gallring i elektronisk miljö.

Gallringsbestämmelserna i den nya lagen bör syfta till att skydda den personliga integriteten för de personer vilkas uppgifter behandlas automatiserat. När elektroniskt material skrivs ut på papper måste detta skydd anses ha uppnåtts och uppgifterna anses gallrade. Varje mindre förändring av den elektroniskt lagrade informationen, t.ex. ändrade sökmöjligheter, kan emellertid inte anses utgöra gallring enligt den nya lagen. Uppgifter kan inte heller anses gallrade enbart genom att de överförts till ett annat datamedium för digital arkivering, eftersom uppgifterna då fortfarande kan bli föremål för olika slag av sammanställningar. Innebörden av de gallringsbestämmelser som föreslås bör vara att uppgifter inte längre ska vara digitalt åtkomliga i verksamheten efter utförd gallring. Uppgifter bör anses gallrade även om de fortfarande förekommer i säkerhetskopierat material eftersom det, som konstateras i betänkandet Säkerhetskopiors rättsliga status, kan vara svårt att åstadkomma att information tas bort vid samma tidpunkt i såväl verksamhets- som säkerhetskopiemiljön (SOU 2009:5 s. 143). Innebörden av gallring berörs även nedan i avsnittet om digital arkivering.

I personuppgiftslagen (1998:204) saknas uttryckliga regler om gallring. Däremot anges i 9 § första stycket i personuppgiftslagen att personuppgifter inte får bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Samtidigt anges i 8 § andra stycket personuppgiftslagen att myndigheternas bevarande av allmänna handlingar inte hindras av lagen. Personuppgiftslagens reglering innebär alltså i den meningen en prioritering av intresset att bevara allmänna handlingar framför integritetsskyddsintresset. En sådan ordning medges också genom punkt 72 i ingressen till dataskyddsdirektivet, som anger att direktivet gör det möjligt att vid genomförandet av bestämmelserna i direktivet ta hänsyn till principen om allmänhetens rätt till tillgång till allmänna handlingar.

Polisdatalagen (1998:622) innehåller flera olika slag av bestämmelser om bevarande och gallring. I 13 § polisdatalagen föreskrivs att uppgifter som inte längre behövs för sitt ändamål ska gallras om inte annat anges i lagen. Regeringen eller den myndighet som regeringen bestämmer får dock meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål. För de särskilda register som förs med stöd av lagen gäller särskilda gallringsfrister. Lagens bestämmelser om gallring gäller inte uppgifter i förundersökningar. Förundersökningar ska i stället bevaras och gallras i den utsträckning som följer av arkivlagen. För de register som förs med stöd av övergångsbestämmelserna till polisdatalagen gäller 12 § i den upphävda datalagen och, i förekommande fall, de särskilda gallringsfrister för respektive register som beslutats av Datainspektionen.

Hur bör regleringen av bevarande och gallring utformas?

Om inga särskilda gallringsbestämmelser föreslås i lagen kommer arkivlagens huvudregel om bevarande att gälla. De bestämmelser om gallring som finns i eller följer av arkivlagen anger när gallring *får* ske och framtvingar alltså inte gallring. När sådana gallringsbestämmelser meddelas är det intresset av offentlighet och insyn som styr frågan om gallring. Arkivlagens bestämmelser om bevarande och gallring syftar således inte till att tillgodose integritetsskyddsintressen.

I polisens brottsbekämpande verksamhet behandlas en stor mängd personuppgifter automatiserat. Som nyss nämnts finns det vid sådan behandling helt andra möjligheter att söka och sammanställa information än när uppgifter behandlas i pappersbaserade system. Detta ökar typiskt sett risken för integritetsintrång. Sekretessbestämmelser och bestämmelser om begränsningar i tillgången till uppgifter kan inte, som *Riksarkivet* hävdar, fullt ut tillgodose integritetsskyddet och ersätta bestämmelser om bevarande och gallring i polisens brottsbekämpande verksamhet. Det bör således finnas regler om bevarande och gallring i den nya lagen. Vid utformningen av sådana bestämmelser bör dock vägas in vilka övriga integritetsskyddande bestämmelser som är tillämpliga, t.ex. begränsningar i fråga om behandling och tillgång till uppgifter. Vidare måste en avvägning göras mellan å ena sidan intresset av skydd för den personliga integriteten och å andra sidan intresset av offentlighet och insyn i myn-

digheternas verksamhet. Som Riksarkivet framhåller är det inte alltid till fördel för en enskild att behandlade personuppgifter gallras.

En första fråga att ta ställning till är om det bör införas en generell bestämmelse i den nya lagen som anger att uppgifter ska gallras när de inte längre behövs för ändamålet med behandlingen. I promemorian övervägdes att införa en sådan bestämmelse men man valde i stället att föreslå särskilda gallringsfrister som anger när gallring senast måste ske. Det konstaterades att en generell bestämmelse om att gallring ska ske då uppgifterna inte längre behövs för ändamålet ger föga ledning i det enskilda fallet, särskilt som en uppgift, insamlad i en viss underrättelseverksamhet eller en viss brottsutredning, så småningom kan visa sig ha betydelse i annan underrättelseverksamhet eller brottsutredning.

Datainspektionen anser att en generell bestämmelse bör införas av innebörd att uppgifter ska gallras när de inte längre behövs för det ändamål för vilket de samlades in och åberopar artikel 5 e i dataskyddskonventionen. Enligt den artikeln får personuppgifter inte bevaras under längre tid än vad som behövs ”for the purpose for which those data are stored”. Datainspektionen anser att uttrycket ska översättas med ”ändamålet för vilket uppgifterna samlades in” och att det torde vara det närmare preciserade ändamålet som avses, till exempel en viss utredning, ett underrättelseprojekt eller liknande. En strikt tillämpning av en sådan bestämmelse torde innebära att alla uppgifter i exempelvis en avslutad förundersökning ska gallras när förundersökningen avslutas, såvida inte uppgifterna bedöms behövas igen för just den förundersökningen.

Datainspektionens uppfattning om hur artikel 5 e i dataskyddskonventionen ska tolkas kan ifrågasättas. I artikeln ställs endast krav på att det ska finnas ett berättigat ändamål för att bevara uppgifter. Av Datainspektionens remissyttrande framgår också att inspektionen anser att det kan vara tillåtet att bevara uppgifter, exempelvis från en avslutad förundersökning, för nya ändamål. Enligt inspektionen synes ett sådant bevarande dock förutsätta att polisen varje gång ett ärende avslutas tar ställning till om någon eller några av uppgifterna i ärendet behövs för något nytt ärende eller projekt. Om inget nytt sådant konkret och avgränsat ändamål skulle finnas vid den tidpunkten synes inspektionen mena att uppgifterna ska gallras. Av inspektionens yttrande framkommer det emellertid även (i ett annat avsnitt än det som avser gallring) att inspektionen menar att uppgifter i en förundersökning alltid bör få uppdatera ”vissa centrala system”.

Brottsbekämpande verksamhet bedrivs i stor utsträckning genom informationsökning, både i polisens egna och i andra myndigheters databaser. Uppgifter i tidigare brottsutredningar och underrättelseärenden får ofta betydelse i senare ärenden, såväl i polisens brottsutredande som brottsförebyggande arbete. När ett ärende avslutas är det ofta mycket svårt att avgöra om, och på vilket sätt, uppgifter i just det ärendet kan komma att få betydelse i något annat ärende hos polisen. Erfarenheterna visar att det är vanligt med återfall i brott, men att man inte på förhand kan avgöra vilka personer som kommer att återfalla eller vilka brott de kommer att begå. Likaså är det väl känt att vissa brottsmönster upprepas, men inte heller där kan man förutse när och var det kommer att inträffa. För att polisen snabbt ska kunna lokalisera gärningsmannen när ett brott begås, måste den kunna dra nytta av sina tidigare erfarenheter och kunskaper

både om brott och om tänkbara gärningsmän. Det förutsätter att polisen i viss utsträckning har tillgång bl.a. till avslutade brottsutredningar, eftersom bara ett fåtal uppgifter är tillgängliga i misstankeregistret och belastningsregistret. På samma sätt som man inom t.ex. hälso- och sjukvården bevarar uppgifter om en persons alla tidigare sjukdomar, utan att man vid den tidpunkten kan förutse om en viss uppgift någonsin kommer att få betydelse för personens framtida medicinska behandling, måste man inom polisen i rimlig utsträckning kunna ta till vara den kunskap som finns inom organisationen kring brott och brottsmisstänkta för den övergripande uppgiften att förebygga, förhindra och utreda brott. Vidarebehandling i form av bevarande under viss tid är således nödvändigt för att polisen ska kunna utföra sina huvuduppgifter.

Ett annat viktigt skäl för att bevara uppgifter i brottsutredningar är att många sådana ärenden avskrivs efter ett summariskt konstaterande att det inte finns något spaningsuppslag eller att brott på det föreliggande materialet inte kan styrkas. Vidare avskrivs många ärenden med stöd av reglerna om s.k. förundersökningsbegränsning, t.ex. därför att personen misstänks för andra brott som antas ge en tillräcklig påföljd. Ärenden av nu aktuellt slag kan behöva tas upp på nytt på grund av ändrade omständigheter, t.ex. att gärningsmannen påträffas eller att nya fakta om brottet kommer fram.

Ett tredje skäl till att uppgifter behöver bevaras en tid efter att ett ärende har avslutats är de behov som ett närarkiv normalt fyller för en myndighet. Man brukar tala om myndighetens behov av ett internt minne.

Utvecklingen inom polisen innebär att ärenden i allt större utsträckning behandlas automatiserat i ärendehanteringssystem. Brottsanmälningar behandlas t.ex. i Rationell anmälningsrutin (RAR) och förundersökningar i Datoriserad utredningsrutin (DurTvå). När polisen behandlar ärenden i pappersbaserade system finns det ett stort behov av att registrera enskilda uppgifter från avslutade ärenden i särskilda personregister för nya ändamål. När uppgifter behandlas automatiserat, t.ex. i ett ärendehanteringssystem för förundersökningar, och när det finns möjlighet att fortsätta att behandla uppgifter i det systemet, är behovet av att skapa särskilda register för nya ändamål mindre. Olika kategorier av uppgifter i ärendena kan i stället göras sökbara där de lagras. Det finns stora fördelar för skyddet av den personliga integriteten med att uppgifter inte bevaras i ett flertal olika register (se avsnitt 6.1).

Det är viktigt att uppgifter bevaras endast om det finns berättigade ändamål för bevarandet. Denna princip kommer till uttryck i artikel 5 e i dataskyddskonventionen. Som nyss redovisats finns det normalt berättigade ändamål för att bevara uppgifter i ett ärende i den brottsbekämpande verksamheten under en tid efter det att ärendet avslutades. Sådant bevarande sker för ett flertal olika ändamål; bevarandet kan sägas ske för mer övergripande brottsbekämpande ändamål. Sådant bevarande bör vara tillåtet även om det alltså inte sker för något särskilt utpekat konkret ändamål, exempelvis en viss brottsutredning. Detta kan sägas innebära en viss skillnad i kravet på ändamålsbestämning mellan behandling av uppgifter i form av bevarande (lagring) av uppgifterna och annan behandling. Annan behandling av uppgifterna än lagring, t.ex. sökning, bör alltid ske för ett visst konkret ändamål.

I sammanhanget bör framhållas att tillgången till lagrade personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Lagrade uppgifter bör också i möjlig mån vara aktuella. Viss uppföljning av avslutade ärenden bör därför krävas (se avsnitt 14.4).

Mot bakgrund av bl.a. kravet i artikel 5 e i dataskyddskonventionen bör – till skillnad från vad som föreslås i promemorian och i likhet med vad *Datainspektionen* anser – den nya lagen enligt regeringens mening innehålla en generell bestämmelse om längsta tid för bevarande. Bestämmelsen bör dock inte utformas på det sätt som inspektionen förordar, eftersom det skulle innebära en för snäv begränsning i polisens möjligheter att behandla uppgifter. I lagen bör föreskrivas att uppgifter inte får bevaras längre än vad som behövs för något eller några av de i lagen angivna ändamålen.

Den nu föreslagna generella bestämmelsen om längsta tid för bevarande ger polisen tämligen vida ramar för bedömningen av vilka uppgifter som får bevaras. Det är framför allt verksamhetsskäl som ska vara styrande för bedömningen av om uppgifterna behövs. För att tillgodose intresset av skydd för den personliga integriteten bör den generella bestämmelsen kompletteras med mer preciserade bestämmelser som föreskriver en yttersta gräns för att bevara vissa kategorier av uppgifter. Sådana bestämmelser bör, som *Datainspektionen* framhåller, utformas utifrån de skilda verksamhetsbehoven av att bevara olika kategorier av uppgifter samtidigt som dessa behov måste vägas mot intresset av att värna den personliga integriteten. Lagens tidsfrister för bevarande och gallring bör utgöra maximifrister. Om det redan vid en tidigare tidpunkt står klart att uppgifterna saknar betydelse från brottsbekämpningssynpunkt ska de gallras eller avskiljas från den brottsbekämpande verksamheten. Detta följer såväl av den nyss föreslagna generella bestämmelsen om längsta tid för bevarande som av föreslagna ändamålsbestämmelser (se avsnitt 7.1–7.5).

De särskilda gallringsbestämmelserna bör, till skillnad mot den generella bestämmelsen, endast gälla automatiserad behandling av personuppgifter. För behandling t.ex. i manuella register behövs inga särskilda gallringsbestämmelser. Motsvarande bedömning gjordes i propositionen Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling (prop. 2004/05:164 s. 94).

Olika gallringsbestämmelser bör gälla beroende på om uppgifterna har gjorts gemensamt tillgängliga eller inte (se avsnitt 14.2 respektive 14.3). Vidare bör särskilda gallringsfrister gälla för uppgifter i de register som föreslås specialregleras i lagen. Ärenden om utredning eller beivrande av brott bör inte omfattas av lagens gallringsbestämmelser. Det bör dock, som promemorian föreslår, finnas bestämmelser som begränsar möjligheten att efter en viss tid behandla uppgifter i brottsanmälningar, förundersökningar och andra brottsutredningar i den brottsbekämpande verksamheten (se avsnitt 14.4). Om uppgifterna fortsätter att behandlas automatiserat för arkivändamål ska de avskiljas från den brottsbekämpande verksamheten (se avsnittet nedan om digital arkivering).

För att tillgodose intresset av offentlighet och insyn bör regeringen eller den myndighet som regeringen bestämmer, utan hinder av bestämmelser om gallring, få meddela föreskrifter om bevarande för historiska,

statistiska eller vetenskapliga ändamål. Frågan om digital arkivering och tillgången till arkiverade uppgifter behandlas i det följande. Regeringen bör även ha möjlighet att meddela föreskrifter om att vissa kategorier av uppgifter ska få behandlas och bevaras under längre tid än de i lagen angivna fristerna. För vissa speciella slag av uppgifter är nämligen fortsatt bevarande befogat (se vidare i avsnitt 14.3 och 14.4).

Som framgått av denna redogörelse är frågor om bevarande och gallring komplexa på grund av motstående intressen. Med anledning av remissynpunkterna har dock regleringen förenklats på olika sätt, både lagtekniskt och materiellt, i förhållande till promemorians förslag.

Datainspektionen gör gällande att den i promemorian föreslagna regleringen inte är förenlig med Sveriges internationella åtaganden. Inspektionen anser bl.a. att de föreslagna fristerna för bevarande inte är tillräckligt preciserade för att uppfylla kraven i artikel 5 e i dataskyddskonventionen och vad som förespråkas i artikel 7:1 andra stycket i Europarådets rekommendation. Som nyss konstaterats innebär artikel 5 e i dataskyddskonventionen att uppgifter inte får bevaras längre än vad som behövs för ändamålet med bevarandet. I den angivna artikeln i Europarådets rekommendation förespråkas bl.a. olika regler för skilda kategorier av uppgifter.

Redan genom att lagen föreslås vara tillämplig endast på behandling av uppgifter i polisens brottsbekämpande verksamhet, och inte exempelvis i polisens förvaltningsverksamhet eller hjälpande verksamhet, kommer olika regler för bevarande att gälla för olika slag av uppgifter inom polisen. I det följande föreslås vidare skilda regleringar för å ena sidan gemensamt tillgängliga uppgifter och å andra sidan uppgifter som inte har gjorts gemensamt tillgängliga. För de register som regleras särskilt i lagen föreslås specifika gallringsfrister. Därutöver föreslås att bevarandet av uppgifter i förundersökningar och andra brottsutredningar ska regleras på ett annorlunda sätt än uppgifter som behandlas i underrättelseverksamhet. I fråga om uppgifter som behandlas i sistnämnda verksamhet föreslås olika gallringsfrister bl.a. beroende på för vilket närmare ändamål uppgifterna behandlas. För uppgifter i en förundersökning föreslås en generell femårig frist. För att sådana uppgifter ska få bevaras under längre tid än fem år krävs detaljerade bestämmelser i förordning som gör skillnad på olika slag av uppgifter och ändamålet för den fortsatta behandlingen.

Sammantaget är en reglering av bevarande och gallring av nu redovisat slag, tillsammans med lagens övriga bestämmelser, väl förenlig med bestämmelserna om bevarande och gallring i de internationella överenskommelser som Datainspektionen åberopar.

Digital arkivering

Rikspolisstyrelsen, Kustbevakningen och *Datainspektionen* väcker frågan om vad som ska gälla för behandlingen av uppgifter från den brottsbekämpande verksamheten som arkiverats digitalt.

Arkivering är ett teknikneutralt begrepp. Handlingar och uppgifter kan således arkiveras digitalt. Som nyss nämnts kan uppgifter som arkiverats fortfarande vara sökbara och tillgängliga i verksamheten. Om endast

arkivlagens bestämmelser skulle vara tillämpliga skulle digitalt arkiverade allmänna handlingar, som inte längre behövs i polisens brottsbekämpande verksamhet, således i princip kunna fortsätta att behandlas på samma sätt som tidigare i verksamheten. Det fortsatta bevarandet skulle dock ske för arkivändamål. Vad som traditionellt avses med gallring och Riksarkivets definition av gallring har redovisats i avsnittet Allmänt om bevarande och gallring.

Bestämmelser i registerförfattningar om gallring av uppgifter och om längsta tid för bevarande syftar till att uppnå nödvändigt integritetsskydd för uppgifterna. Om uppgifterna även efter föreskrivna frister får behandlas på samma sätt som tidigare uppnås inte det avsedda skyddet.

Som föreslås i promemorian bör brottsanmälningar, förundersökningar och andra brottsutredningar inte gallras utan, liksom enligt gällande rätt, få bevaras för arkivändamål med stöd av arkivlagen när de inte längre behövs i den brottsbekämpande verksamheten. Mot bakgrund av att arkivlagen inte hindrar eller ställer upp några begränsningar för fortsatt digital behandling av arkiverade uppgifter i den brottsbekämpande verksamheten, behövs det närmare föreskrifter som anger ramen för sådan fortsatt behandling för att skapa nödvändigt integritetsskydd.

Vad gäller uppgifter som ska gallras enligt den nya lagen har *Rikspolisstyrelsen,* under åberopande av Riksarkivets definition av gallring, tolkat promemorians förslag på det sättet att även utgallrade uppgifter får bevaras i ett digitalt arkiv i verksamheten. Detta kan inte ha varit avsikten med förslaget. Som nämnts inledningsvis bör syftet med och innebörden av de gallringsbestämmelser som föreslås vara att uppgifter i princip inte längre ska vara digitalt åtkomliga i verksamheten efter utförd gallring. Uppgifter som omfattas av lagens gallringbestämmelser kan dock komma att arkiveras digitalt om regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om bevarande för historiska, vetenskapliga eller statistiska ändamål.

Föreskrifter som anger ramen för behandlingen av digitalt arkiverade uppgifter meddelas lämpligen i förordning. Digitalt arkiverade uppgifter som inte längre får behandlas i den brottsbekämpande verksamheten bör avskiljas genom att uppgifterna bevaras i en separat databas eller genom någon liknande åtgärd. Bestämmelserna i arkivlagen om arkivbildning och dess syften samt arkivlagens bestämmelser om arkivvård bör vara avgörande för hur informationen bevaras och struktureras. Som en följd av detta bör det i första hand vara tjänstemän vid myndighetens arkiv som har direkt tillgång till uppgifterna.

14.2 Gallring av uppgifter som inte har gjorts gemensamt tillgängliga

Regeringens förslag: Personuppgifter som inte har gjorts gemensamt tillgängliga ska gallras senast ett år efter det att de behandlades automatiserat första gången eller, om de har behandlats i ett ärende, senast ett år efter det att ärendet avslutades.

Utredningens förslag innehåller inte några särskilda gallringsbestämmelser för uppgifter som inte har gjorts gemensamt tillgängliga. Personuppgifter ska enligt utredningens förslag gallras när de inte längre behövs för ändamålet med behandlingen.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna har inte yttrat sig särskilt i frågan om gallring av uppgifter som inte har gjorts gemensamt tillgängliga.

Skälen för regeringens förslag: Från integritetssynpunkt är det viktigt att personuppgifter inte behandlas längre än nödvändigt och att det utöver en generell bestämmelse om längsta tid för bevarande finns särskilda gallringsfrister för olika kategorier av uppgifter som behandlas automatiserat. När gallringsfristernas längd bestäms finns det anledning att göra skillnad mellan uppgifter som har gjorts gemensamt tillgängliga och andra uppgifter. När det gäller uppgifter som inte har gjorts gemensamt tillgängliga, torde behovet av att behandla dem under längre tid typiskt sett vara begränsat. Dessutom är det från integritetssynpunkt särskilt angeläget att sådana uppgifter inte behandlas under längre tid, eftersom det enligt förslaget endast kommer att gälla ett fåtal begränsningar för behandlingen av dem. Det bör därför uppställas särskilt korta gallringsfrister för uppgifter som inte har gjorts gemensamt tillgängliga.

När det gäller uppgifter som behandlas inom ramen för ett ärende bör gallring lämpligen ske inom ett år efter det att ärendet avslutades. Uppgifter som inte kan hänföras till ett ärende bör i stället gallras inom ett år efter det att uppgifterna behandlades första gången. Gränsdragningen mellan de båda fallen redovisas i författningskommentaren. I likhet med vad som föreskrivs i polisdatalagen bör det finnas en möjlighet för regeringen att föreskriva att uppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål (se avsnitt 14.1).

När uppgifter behandlas i ärenden om utredning eller beivrande av brott, gör sig dock särskilda hänsyn gällande. De nu föreslagna gallringsfristerna bör därför inte gälla uppgifter i sådana ärenden. Den frågan behandlas i avsnitt 14.4.

14.3 Gallring av gemensamt tillgängliga uppgifter

Regeringens förslag: Personuppgifter som har gjorts gemensamt tillgängliga och som kan antas ha samband med brottslig verksamhet ska som huvudregel gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Vid allvarlig brottslig verksamhet är tidsfristen i stället fem år.

Personuppgifter som har behandlats i samband med övervakning av brottsbelastade eller potentiellt farliga personer ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Den tid då en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av respektive gallringsfrist.

Uppgifter som har behandlats inom ramen för det internationella samarbetet ska gallras senast ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Uppgifter som har behandlats enbart på den grunden att de har rapporterats till polisens kommunikationscentraler ska gallras senast ett år efter utgången av det kalenderår då rapporteringen gjordes.

Utredningens förslag: Personuppgifter som behandlas automatiserat och som avser en enskild person mot vilket det inte finns någon misstanke om brott ska få bevaras högst tre år från det att uppgifterna om personen samlades in. Uppgifter om övervakade personer ska dock få bevaras så länge personen är noterad i belastningsregistret. Vidare föreslås särskilda gallringsregler för det spaningsregister som utredningen har föreslagit och för DNA-register och fingeravtrycks- och signalementsregister. I de fall där inga särskilda gallringsregler gäller ska enligt förslaget gallring ske om personuppgifterna inte längre behövs för ändamålet med behandlingen.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot dem. *Rikspolisstyrelsen* har ansett att den föreslagna gallringsfristen om tre år är alltför kort.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås dock ingen längre gallringsfrist om fem år för uppgifter om allvarlig brottslig verksamhet. Däremot föreslås en fast gallringsfrist för uppgifter om personer som inte är misstänkta.

Remissinstanserna: Flertalet av remissinstanserna tillstyrker eller har inget att invända mot förslaget. *Riksdagens ombudsmän* anser att de verksamhetsmässiga behov som anförs till stöd för en gallringsfrist om tio år för uppgifter om övervakade personer inte står i proportion till den integritetskränkning som behandling av uppgifterna under så lång tid innebär. *Justitiekanslern* ifrågasätter om den föreslagna gallringsbestämmelsen för uppgifter om personer som inte misstänkts för något konkret brott tillgodoser kraven på behovsprövning i dataskyddskonventionen.

Rikspolisstyrelsen anser att gallringstiderna i vissa fall bör förlängas. Styrelsen anser bl.a. att de föreslagna gallringsbestämmelserna beträf-

fande uppgifter om personer som inte är eller har varit misstänkta respektive personer som inte är eller har varit övervakade måste ändras så att gallringsreglerna för dessa kategorier av uppgifter är desamma som för uppgifter om misstänkta respektive övervakade personer. De föreslagna gallringsbestämmelserna skulle enligt styrelsen försvåra och i vissa fall omöjliggöra polisens långsiktiga underrättelsearbete. Styrelsen framhåller att det ligger i polisens eget intresse att inte ha inaktuella uppgifter och att gallring av uppgifter om personer som inte är misstänkta därför många gånger kommer att ske oftare än i samband med gallring av uppgifterna om den misstänkte. Styrelsen väcker även frågan om hur gallringsbestämmelserna ska tillämpas på löpande text och på bild- och ljudupptagningar. Rikspolisstyrelsen framhåller vidare att kartläggning av den grova organiserade brottsligheten är komplex och tidskrävande och att sådant arbete i stor utsträckning sker i s.k. särskilda undersökningar. Enligt styrelsen ger de föreslagna gallringsbestämmelserna inte samma utrymme att bevara uppgifter i den typen av uppgiftssamlingar som gällande regler.

Datainspektionen anser att de föreslagna gallringsbestämmelserna inte är tillräckligt preciserade och att de därför inte uppfyller kraven i artikel 5 e i dataskyddskonventionen. Inspektionen hänvisar även till artikel 7:1 andra stycket i Europarådets rekommendation om användning av personuppgifter inom polissektorn.

Riksarkivet framhåller att det är viktigt att regeringen utnyttjar möjligheten att bemyndiga Riksarkivet att meddela föreskrifter om att uppgifter som enligt lagen ska gallras får bevaras för arkivändamål.

Skälen för regeringens förslag

Särskilda gallringsfrister

Särskilda gallringsfrister bör bestämmas för uppgifter som har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. Ärenden om utredning eller beivrande av brott bör dock inte omfattas av lagens gallringsbestämmelser. I stället bör särskilda bestämmelser införas som begränsar möjligheterna att behandla uppgifterna i den brottsbekämpande verksamheten. Den frågan tas upp i avsnitt 14.4.

Bestämmelser med särskilda gallringsfrister kompletterar den generella bestämmelsen om bevarande (se avsnitt 14.1). Sådana bestämmelser anger tidpunkten för när en uppgift måste gallras av integritetsskäl, trots att det fortfarande kan finnas verksamhetsintressen som talar för att bevara uppgiften.

I en så mångfasetterad verksamhet som polisens kommer det, oavsett hur man utformar gallringsbestämmelserna, att finnas vissa situationer där de särskilda gallringsbestämmelserna fungerar mindre väl. Vissa kategorier av uppgifter bör därför kunna få behandlas under längre tid än de frister som föreslås nedan, exempelvis sådana uppgifter som behandlas i polisens digitala register över barnpornografiska bilder. Regeringen bör därför få meddela föreskrifter om att vissa kategorier av uppgifter, ska få behandlas och bevaras under längre tid (se avsnitt 14.1). Sådana föreskrifter bör dock meddelas endast i begränsad utsträckning och vara preciserade. De närmare ändamålen för bevarandet bör anges liksom när

uppgifterna senast ska gallras. Regeringen eller den myndighet som regeringen bestämmer bör också få meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål (se avsnitt 14.1).

En viktig fråga är vilken gallringsfrist som ska gälla om uppgifter som har samlats in i visst sammanhang före gallringsfristens utgång används i ett annat projekt eller ärende. Vad bör t.ex. gälla om uppgifter, som har rapporterats till polisens kommunikationscentral, kort tid efter rapporteringen tas tillvara i ett underrättelseprojekt? Bör den ursprungliga gallringsfristen gälla eller bör man tillämpa den gallringsfrist som gäller för underrättelseprojektet? Enligt regeringens mening bör man, som promemorian föreslår, tillämpa den gallringsfrist som gäller för uppgiften i dess nya sammanhang. Uppgifter i ett underrättelseprojekt som har inhämtats via polisens kommunikationscentral bör alltså gallras enligt samma principer som gäller för uppgifter som har inhämtats på annat sätt.

Rikspolisstyrelsen väcker frågan om hur gallringsbestämmelserna ska tillämpas på löpande text och på bild- och ljudupptagningar. Denna fråga får framför allt betydelse när uppgifter i samma handling eller bild- och ljudupptagning innehåller uppgifter om flera personer och det gäller olika gallringstider för uppgifter som rör dessa. Eftersom skälet för bevarandet torde kunna knytas till viss person bör utgångspunkten vara att handlingen eller upptagningen får bevaras så länge uppgifter om den personen får bevaras, under förutsättning att bevarandet behövs.

Datainspektionens invändning att de i promemorian föreslagna gallringsfristerna som anger längsta tid för bevarande inte är tillräckligt preciserade bemöts i avsnitt 14.1.

Uppgifter om personer som antas ha samband med brottslig verksamhet

Gemensamt tillgängliga uppgifter som kan antas ha samband med misstänkt brottslig verksamhet bör normalt gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Detta överensstämmer i stort med vad som för närvarande gäller för gallring av uppgifter i kriminalunderrättelseregister (21 § polisdatalagen) och i den s.k. tullbrottsdatabasen (27 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet). Den föreslagna gallringsfristen gör det möjligt för polisen att behålla uppgifter beträffande s.k. mängdbrottslighet – där det är vanligt med återfall – tillräckligt länge. Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning bör inte räknas in i gallringsfristen.

Rikspolisstyrelsen anser att polisen behöver bevara vissa uppgifter i underrättelseverksamheten längre än tre år från det att registreringen gjordes. Styrelsen framhåller bl.a. att polisen har stort behov av att även fortsättningsvis arbeta i s.k. särskilda undersökningar och gör gällande att de föreslagna gallringsbestämmelserna inte ger samma utrymme som nu att bevara uppgifter i den typen av uppgiftssamlingar. Styrelsen föreslår att uppgifter i ett ärende ska gallras senast ett år efter det att ärendet avslutades.

Det är viktigt att polisen även fortsättningsvis har möjlighet att arbeta i särskilda underrättelseprojekt, bl.a. för att kunna inrikta verksamheten på

viss kriminell gruppering eller verksamhet, exempelvis mc-brottslighet. Som styrelsen framhåller bevarar polisen med stöd av gällande bestämmelser vissa särskilda undersökningar under längre tid än tre år genom att man varje år fattar särskilda beslut om förlängning av gallringsfristen (se 16 § polisdatalagen). Detta gäller framför allt särskilda undersökningar som avser grov brottslighet.

Med en sådan gallringsbestämmelse som Rikspolisstyrelsen föreslår skulle uppgifter kunna komma att bevaras under en alltför lång tid, bl.a. med hänsyn till att vissa underrättelseprojekt kan pågå länge. I princip skulle vissa underrättelseprojekt aldrig behöva avslutas. Detta vore inte godtagbart från integritetssynpunkt. Ett alternativ vore att införa en bestämmelse som liknar 16 § polisdatalagen, som reglerar gallringen av uppgifter i särskilda undersökningar. De särskilda undersökningarna bör emellertid, som föreslås i promemorian, inte regleras särskilt i den nya lagen (se även avsnitt 7.2). I stället för att koppla gallringen till visst ärende, projekt eller undersökning bör gallringsfristerna, på det sätt som föreslås i promemorian, knytas till de personuppgifter som behandlas.

För att tillgodose bl.a. de behov som polisen har av att behandla uppgifter i särskilda underrättelseprojekt bör en förlängning av den föreslagna treåriga gallringfristen övervägas. Det är, om man jämför med dagens regler och vad som gäller för tullbrottsdatabasen, inte motiverat med en generell förlängning, utan en längre gallringsfrist bör omfatta endast uppgifter som har samband med allvarlig brottslig verksamhet. Ju allvarligare brottslighet det är fråga om, desto mer befogat är det att kunna bevara uppgifter längre. Som redovisas närmare i avsnittet om uppgifter som behövs för övervakningen av vissa personer behöver polisen kunna bevara uppgifter under en relativt lång tid i arbetet med att bekämpa den grova organiserade brottsligheten. Ett av skälen för detta är att det inte är ovanligt att misstänkta personer håller sig undan i flera år, kanske för att uppgifterna om dem ska hinna gallras ur polisens system. Frågan är då hur lång tid uppgifter om allvarlig brottslig verksamhet bör få bevaras. För uppgifter som behandlas i samband med övervakning föreslås en gallringsfrist om tio år. Den tioåriga gallringsfristen kommer emellertid att omfatta endast viss behandling för att komma till rätta med den grova organiserade brottsligheten och bara beröra ett mycket begränsat antal personer. En så lång bevarandetid är enligt regeringens mening inte rimlig för uppgifter i annan underrättelseverksamhet, även om den avser allvarlig brottslig verksamhet.

En samlad bedömning ger vid handen att det bör gälla två olika gallringsfrister för uppgifter som kan antas ha samband med brottslig verksamhet. Utöver den treåriga fristen som föreslås i promemorian bör det införas en längre gallringsfrist om fem år för uppgifter som kan antas ha samband med allvarlig brottslig verksamhet.

Justitiekanslern ifrågasätter om den i promemorian föreslagna gallringsbestämmelsen uppfyller kravet på behovsprövning i dataskyddskonventionen, eftersom gallring inte synes behöva ske förrän efter tre år. Som framgått ovan är dataskyddskonventionens krav uppfyllt bl.a. mot bakgrund av att det numera även föreslås en generell bestämmelse om längsta tid för bevarande (se avsnitt 14.1).

Rikspolisstyrelsen är kritisk mot förslaget om en fast gallringsfrist om tre år för uppgifter om icke-misstänkta personer och anser att samma frist

bör gälla för dessa uppgifter som för uppgifter om misstänkta och övervakade personer. Styrelsen hävdar bl.a. att polisens långsiktiga underrättelsearbete skulle försvåras och i vissa fall omöjliggöras med föreslagna gallringsbestämmelser. Enligt styrelsen riskerar samtliga uppgifter om en misstänkt person att bli oanvändbara om uppgifter exempelvis om fordon och vistelseadresser som denne använder, men som tillhör någon annan, skulle behöva gallras före uppgifterna om den misstänkte. Rikspolisstyrelsen har även svårt att se hur polisen ska hantera de olika gallringsfristerna rent praktiskt.

De skäl som polisen framför till stöd för att bevara uppgifter om icke-misstänkta under längre tid än tre år är värda att beakta. I sammanhanget bör också vägas in att det i underrättelseverksamhet – i motsats till vid brottsutredning – inte finns någon klart definierad grad av misstanke och att skillnaden därför kan vara liten mellan den som betecknas som misstänkt och andra personer vilkas uppgifter behandlas som ett led i underrättelseverksamheten. Verksamhetsskäl talar därför mot att ha en särskild gallringsbestämmelse utformad så som föreslagits i promemorian. Dessa skäl måste dock vägas mot integritetsskyddsintressen. Vid denna intresseavvägning bör beaktas att en stor del av behandlingen av nu aktuella uppgifter får anses vara mindre känslig. Många av de uppgifter som behandlas finns t.ex. redan tillgängliga i offentliga register, exempelvis uppgifter om anhöriga. Risken för integritetsintrång är därmed begränsad. Det rör sig också i stor utsträckning om indirekta personuppgifter, t.ex. namn på tidigare arbetsgivare, registreringsnummer på bilar som iakttagits i samband med en misstänkt person, telefonnummer som denne varit i kontakt med och uppgifter om bostäder där en misstänkt person brukar uppehålla sig. Ofta är det fråga om att en person nämns i ett tips som lämnats till polisen, exempelvis att den misstänkte personen befunnit sig på fest hos personen i fråga eller suttit i samma bil. Sådana uppgifter kan ha stort polisiärt värde och det kan inte anses oproportionerligt att bevara dem en tid.

Trots att en uppgift i många fall framstår som harmlös är uppgifter om personer som inte är misstänkta emellertid särskilt skyddsvärda och bör enligt regeringens mening kringgärdas av integritetsskyddande bestämmelser. Därför föreslås bl.a. att det ska framgå att personen inte är misstänkt och att uppgifterna ska omfattas av sökbegränsningar (se avsnitt 10 och 11). Detta är av stort värde ur integritetsskyddssynpunkt och bör tas med vid bedömningen av när uppgifterna bör gallras. Vidare bör vägas in den föreslagna generella bestämmelsen om längsta tid för bevarande som naturligtvis är tillämplig även för nu aktuella uppgifter.

Det kan övervägas om man bör införa en gallringsbestämmelse som kräver att polisen efter tre år omprövar behovet av att bevara den aktuella uppgiften. Mot bakgrund bl.a. av den stora mängd uppgifter ett underrättelseprojekt kan innehålla, t.ex. uppgifter om telefonnummer, skulle en sådan ordning lägga en stor administrativ börda på polisen. Det får anses tillräckligt med det krav på att löpande ompröva behovet av att bevara uppgifter som följer av andra bestämmelser i lagen. Dessutom har polisen, som *Rikspolisstyrelsen* framhåller, ett eget intresse av att gallra inaktuella uppgifter. Gallring av uppgifter om personer som inte är misstänkta kommer därför enligt styrelsen många gånger att ske oftare än i samband med gallring av uppgifterna om den misstänkte. En samlad

bedömning ger vid handen att det inte bör införas någon särskild gallringsfrist för uppgifter om icke-misstänkta personer.

Uppgifter som behövs för övervakningen av personer

Som både Polisdatautredningen och promemorian menar är en gallringsfrist om tre år – och även den nu föreslagna femårsfristen – alltför kort när det gäller personuppgifter som behandlas för övervakning av grovt kriminella personer. Utredningen föreslår att sådana personuppgifter ska kunna bevaras så länge uppgifter om den övervakade personen fortfarande finns i belastningsregistret. För belastningsregistret gäller olika gallringsfrister, beroende på vilket brott den aktuella personen har dömts för. Enligt regeringens mening bör man inte välja den lösningen, dels därför att en sådan ordning skulle bli svåröverskådlig, dels därför att det inte är givet att alla de personer som är föremål för övervakning finns i belastningsregistret. Gallringsfristen kan också bli för lång om personen gör sig skyldig till upprepade nya brott av mindre allvarligt slag. I stället bör, i enlighet med promemorians förslag, en gallringsfrist om tio år gälla för uppgifter som behandlas för att de behövs för övervakningen av en person. Fristen bör räknas från utgången av det kalenderår då den senaste registreringen gjordes. Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning bör inte räknas in i gallringsfristen.

Riksdagens ombudsmän anser att de verksamhetsskäl som anförs till stöd för en gallringstid om tio år inte står i proportion till den integritetskränkning som en behandling av uppgifter under så lång tid innebär. Man skulle i och för sig kunna överväga en något kortare gallringsfrist, exempelvis fem eller sju år. Det som kan sägas tala för detta, utöver en minskad risk för integritetsintrång, är att fristen för gallring föreslås automatiskt förlängas om det tillkommer nya uppgifter om den registrerade (se nedan). Mot en kortare frist talar framför allt verksamhetens behov. Det kan ta avsevärd tid att bygga upp kunskap om exempelvis personer som finansierar allvarlig brottslighet eller om de nätverk och strukturer i vilka det bedrivs organiserad brottslighet. Erfarenheterna visar också att brottslig verksamhet som bedrivs i mer eller mindre organiserade former normalt måste övervakas under en avsevärd tid innan man har tillräckligt underlag för att ingripa mot huvudmännen. Det är inte heller ovanligt att personer som misstänks för att utöva allvarlig brottslig verksamhet håller sig undan, t.ex. vistas utomlands, under längre perioder. I sådana fall är det av stort värde för polisen att kunna ha kvar information om personen i fråga om denne fortsätter eller återupptar brottsligheten i Sverige.

Vid avvägningen mellan verksamhetsintressen och integritetsskyddsintressen är det viktigt att komma ihåg dels att det är få personer som kommer i fråga för övervakning av nu aktuellt slag och att det typiskt sett rör sig om personer som polisen misstänker livnär sig på grov brottslighet, dels att tillgången till behandlade uppgifter kommer att vara starkt begränsad inom polisen. Bekämpningen av grov och organiserad brottslighet är högt prioriterad. En alltför kort gallringsfrist skulle motverka syftet med behandlingen. En tioårig gallringsfrist är därför inte oproportionerlig när man beaktar de skadeverkningar för samhället och enskilda

som sådan brottslighet orsakar. Gallringsfristen stämmer överens med vad som föreslås gälla för Säkerhetspolisens behandling av personuppgifter. Det är också viktigt att framhålla att den föreslagna generella bestämmelsen om längsta tid för bevarande är tillämplig. Uppgifter som inte behövs för något eller några av lagens ändamål får inte fortsätta att behandlas, trots att tioårsfristen inte har löpt ut.

Sammantaget utgör en tioårig gallringsfrist en rimlig avvägning mellan verksamhetsintressen och integritetsskyddsintressen. Någon särskild gallringsfrist bör inte gälla för uppgifter om personer som inte själva står under övervakning. Skälen för detta är desamma som redovisas vad gäller gallring av uppgifter som rör icke-misstänkta personer.

Uppgifter som behandlas inom ramen för det internationella samarbetet

Allt arbete som görs för att fullgöra internationella åtaganden är i princip ärendebaserat. När en förfrågan kommer från ett annat land hanteras denna inom ramen för någon form av ärende. Polisen behöver bevara sådana ärenden en tid efter det att ärendet har avslutats bl.a. för att i efterhand kunna svara på frågor om vidtagna åtgärder. I promemorian föreslås att uppgifterna i ärendet ska gallras senast ett år efter det att ärendet har avslutats. *Rikspolisstyrelsen* anser att internationella ärenden behöver bevaras längre än ett år efter det att ärendet avslutades bl.a. på grund av att det inte är ovanligt att ett land återkommer med ytterligare frågor i ett ärende efter mer än ett år. I avsnitt 15.5 föreslås en särreglering av Rikspolisstyrelsens internationella register. Genom detta förslag tillgodoses det behov av att kunna återfinna avslutade ärenden som styrelsen påtalar. För registret föreslås en gallringstid om tre år. Den i promemorian föreslagna gallringstiden om ett år bör dock gälla för sådan behandling av personuppgifter i internationella ärenden som inte sker i nyss nämnda register. Fristen bör dock – på samma sätt som övriga gallringsfrister för gemensamt tillgängliga uppgifter – räknas från utgången av det kalenderår då ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som rapporterats till polisens kommunikationscentraler

Rikspolisstyrelsen anser att den föreslagna gallringsbestämmelsen för uppgifter som rapporterats till polisens kommunikationscentraler behöver analyseras närmare i den fortsatta beredningen. Styrelsen pekar bl.a. på att enskilda riskerar att sakna dokumentation från polisen över trafikolyckor om uppgifter gallras redan efter ett år.

Uppgifter som har rapporterats till polisens kommunikationscentraler bör kunna göras gemensamt tillgängliga, oavsett uppgifternas karaktär. Behovet av att behandla uppgifter i den verksamheten består dock normalt enbart under en kortare tid. Om uppgifterna tillförs en brottsutredning ska bestämmelserna om bevarande och behandling av sådana uppgifter tillämpas. Promemorians bedömning att uppgifter som rapporteras till polisens kommunikationscentraler bör gallras senast ett år efter rapporteringen är rimlig. Förslaget synes i huvudsak överensstämma med hur polisen använder sig av uppgifter i det datasystem som för närvarande används i kommunikationscentralerna (KC-systemet, se *bilaga 6*).

Såvitt känt är det mycket ovanligt att uppgifter hämtas från det digitala lagringsmedium där uppgifterna lagras i ytterligare fem år efter att gällande frist om 13 månader löpt ut. De omständigheter som Rikspolisstyrelsen framför till stöd för en längre gallringsfrist är inte heller sådana att de kan anses motivera en längre tid för bevarande än ett år, särskilt mot bakgrund av att det rör sig om ett stort antal uppgifter som berör många personer. Fristen bör dock – på samma sätt som övriga gallringsfrister avseende gemensamt tillgängliga uppgifter – räknas från utgången av det kalenderår då uppgifterna behandlades första gången.

14.4 Ärenden om utredning eller beivrande av brott

Regeringens bedömning: Det bör inte införas några särskilda gallringsbestämmelser för uppgifter i ärenden om utredning eller beivrande av brott. Det bör däremot föreskrivas vissa begränsningar i möjligheten att behandla uppgifter i brottsanmälningar, förundersökningar eller andra utredningar som handläggs enligt 23 kap. rättegångsbalken i den brottsbekämpande verksamheten. Begränsningarna bör dock inte hindra att uppgifterna arkiveras eller gallras enligt arkivlagens bestämmelser.

Regeringens förslag: För personuppgifter i brottsanmälningar, avslutade förundersökningar och andra liknande utredningar som har gjorts gemensamt tillgängliga ska följande begränsningar gälla för behandlingen.

Om en förundersökning har lagts ned, om åtal har lagts ned eller om den misstänkte har frikänts genom en dom som har vunnit laga kraft, ska personen inte vara sökbar som misstänkt.

Personppgifter i en brottsanmälan, som inte har lett till förundersökning eller annan motsvarande utredning, får inte behandlas i polisens brottsbekämpande verksamhet när det brott som anmälan avser har preskriberats. Uppgifter i en anmälan som avser ett handlande som inte har bedömts utgöra brott ska över huvudtaget inte få behandlas.

Personuppgifter i förundersökningar och liknande brottsutredningar ska inte heller få behandlas i polisens brottsbekämpande verksamhet 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.

När de angivna tidsfristerna har löpt ut ska uppgifter i en förundersökning få behandlas endast om

1. uppgiften behövs för något nytt enligt lagen tillåtet konkret ändamål, t.ex. i en annan förundersökning eller i en undersökning av viss brottslig verksamhet, eller
2. uppgiften får behandlas längre enligt föreskrifter som har meddelats av regeringen.

Utredningens bedömning och förslag överensstämmer delvis med promemorians. Utredningen föreslår dock inte någon särskild bestämmelse om behandling av uppgifter i brottsanmälningar eller om behand-

ling av sådana uppgifter i förundersökningar eller liknande brottsutredningar som inte utgör uppgifter om brottsmisstanke.

Remissinstanserna: Flertalet remissinstanser har inte haft någon invändning mot utredningens förslag. *Rikspolisstyrelsen* har föreslagit att behandling av kvarstående misstankar ska vara tillåten även i andra fall, om det finns särskilda skäl. Rikspolisstyrelsen har hänvisat till att uppgifterna i en nedlagd förundersökning kan vara av stort värde i arbetet med att kartlägga den organiserade brottsligheten. Styrelsen har också pekat på behovet av att kunna behandla uppgifter om kvarstående misstankar som gäller brott mot kvinnor som lever under hot.

Promemorians bedömning och förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot bedömningen eller förslaget. *Riksarkivet* stöder bedömningen att arkivlagens bestämmelser ska vara tillämpliga på bevarandet av brottsanmälningar, förundersökningar och andra brottsutredningar. Även *Åklagarmyndigheten* delar promemorians bedömning att det inte bör införas några gallringsbestämmelser för uppgifter i förundersökningar. Myndigheten anser dock att bestämmelserna med inskränkningar i möjligheterna att behandla sådana uppgifter är svårtillgängliga och att det bör finnas utrymme för förenklingar. Åklagarmyndigheten, liksom *Rikspolisstyrelsen*, framhåller vikten av att kunna hitta en nedlagd förundersökning genom att söka på en tidigare misstänkt persons personnummer och efterlyser förtydliganden av innebörden av den föreslagna bestämmelsen om att en person inte får vara sökbar som misstänkt sedan en förundersökning har lagts ned eller avslutats på något annat sätt. Vad gäller den föreslagna bestämmelsen om behandling av brottsanmälningar efterfrågar *Åklagarmyndigheten* förtydliganden i fråga om vad som avses med att den påstådda gärningen inte utgör brott. Myndigheten är också mycket tveksam till förslaget om att beslut att lägga ned en förundersökning ska förenas med en förklaring från beslutsfattaren om att brottet ändå kan komma att bli föremål för lagföring. Enligt Åklagarmyndigheten är det olämpligt att som en del av ett individuellt beslut samtidigt förmedla till de berörda att den utpekade fortfarande är misstänkt.

Rikspolisstyrelsen anser att polisen behöver ha tillgång till uppgifter i avslutade förundersökningar under längre tid än fem år efter dom eller beslut med anledning av domstolsprövning. Uppgifterna behövs exempelvis i samband med utredning av seriebrott såsom sexualbrott, rån och mord, för att kunna gå tillbaka till äldre undersökningar och jämföra modus operandi, finna fastlagda kontakter mellan personer och deras kännedom om t.ex. geografiska förhållanden m.m. Enligt styrelsen bör uppgifter i en förundersökning eller liknande utredning som lett till fällande dom få behandlas i den brottsbekämpande verksamheten så länge domen finns antecknad i belastningsregistret. Även uppgifter i nedlagda förundersökningar behöver enligt Rikspolisstyrelsen kunna behandlas längre än de fem år från nedläggningsbeslutet som föreslås i promemorian. Polisen behöver sådana uppgifter bl.a. för att genomföra sökningar på modus operandi, att förstå om brotten är systematiska, eskalerande beträffande våldsanvändning, utförda mot en särskild målgrupp (etnisk tillhörighet, homosexuella o.s.v.) och vid genomförandet av hot- och riskbedömningar med anledning av nya anmälningar. Uppgifter i

nedlagda förundersökningar behövs inte bara om det aktuella brottet kan komma att bli föremål för lagföring i framtiden utan kan även behövas för att man ska lyckas bättre med en ny förundersökning avseende ett annat brott. Uppgifter i en nedlagd förundersökning kan också vara till fördel för en misstänkt person som blir misstänkt i en ny förundersökning. Rikspolisstyrelsen anser att uppgifterna bör få behandlas till dess brotten preskriberas.

Rikspolisstyrelsen anser vidare att särskilda överväganden behövs i fråga om behandling av uppgifter om tillgripet gods, eftersom sådana uppgifter behöver kunna behandlas längre än vad som föreslås i promemorian. Polisen har bl.a. ett stort behov av att kunna söka uppgifter om stulet gods, t.ex. tavlor eller vapen, även efter det att brottet har preskriberats.

Datainspektionen anser att de förslagna bestämmelserna inte är tillräckligt preciserade och att de därför inte uppfyller de krav som följer av artikel 5 e i dataskyddskonventionen. Inspektionen hänvisar även till artikel 7:1 andra stycket i Europarådets rekommendation om användning av personuppgifter inom polissektorn.

Skälen för regeringens bedömning och förslag

Inga gallringsbestämmelser för förundersökningar

Polisdatalagen skiljer på gallring av uppgifter i förundersökningar och gallring av andra personuppgifter. Förundersökningar arkiverades redan före polisdatalagens tillkomst enligt arkivlagstiftningen och frågan om gallring av förundersökningar avgjordes därmed av det regelverket. I förarbetena till polisdatalagen uttalades att frågan om gallring inte bör vara beroende av vilka tekniska hjälpmedel polisen väljer för sitt arbete (prop. 1997/98:97 s. 109). Det ansågs att uppgifter som behandlas automatiserat i en förundersökning bör hanteras på samma sätt som motsvarande uppgifter som hanterats manuellt. Förundersökningsuppgifter som behandlas automatiserat omfattas alltså inte av polisdatalagens gallringsbestämmelser.

Skälen bakom den nuvarande ordningen gör sig fortfarande gällande. De skäl som *Riksarkivet* för fram till stöd för att uppgifter bör kunna bevaras för arkivändamål har särskild tyngd i fråga om brottsutredningar och liknande ärenden. Därför föreslås inte några särskilda gallringsbestämmelser i fråga om personuppgifter i ärenden om utredning eller beivrande av brott. I promemorian och Polisdatautredningen föreslås ett motsvarande undantag.

Om en uppgift från en brottsutredning behandlas för ett annat ändamål, t.ex. i ett underrättelseprojekt, bör dock, som tidigare nämnts, uppgifterna i det sammanhanget gallras enligt de gallringsbestämmelser som gäller för sådan behandling.

En möjlighet att utan några begränsningar behandla uppgifter i alla avslutade brottsutredningar skulle emellertid kunna innebära stora integritetsrisker. I avsaknad av särskilda gallringsbestämmelser bör det därför gälla begränsningar bl.a. i fråga om hur länge uppgifter i en förundersökning får vara tillgängliga i den brottsbekämpande verksamheten. Dessa begränsningar – som kompletterar den generella bestämmelsen om

längsta tid för bevarande – bör endast gälla gemensamt tillgängliga uppgifter och bör inte hindra att uppgifterna arkiveras eller gallras enligt bestämmelserna i arkivlagen. För att uppnå det integritetsskydd som eftersträvas med bestämmelser om tidsbegränsning av behandlingen av uppgifter i den brottsbekämpande verksamheten bör regeringen också meddela kompletterande föreskrifter om att uppgifter som arkiveras digitalt ska avskiljas (se avsnitt 14.1 där frågan om digital arkivering behandlas).

Behandling av uppgifter om brottsmisstankar

I 10 och 11 §§ polisdatalagen finns det särskilda bestämmelser om behandling av uppgifter om brottsmisstankar som förekommer i avslutade förundersökningar. En sådan uppgift får, om förundersökningen har lagts ned på grund av bristande bevisning, behandlas enbart om den misstänkte fortfarande bedöms vara skäligen misstänkt för brottet och uppgifterna behövs för att förundersökningen ska kunna tas upp på nytt. Har åtal mot personen lagts ned eller ogillats, får uppgiften behandlas för annat ändamål än arkivering endast om förundersökningen tas upp på nytt eller för prövning av om resning bör ske. Motsvarande bestämmelser finns i 17 och 18 §§ lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

En utgångspunkt bör vara att den nya lagen ska innehålla bestämmelser som fyller en liknande funktion som reglerna i 10 och 11 §§ polisdatalagen, vilket också föreslås i promemorian. Av hänsyn till enskildas integritet bör givetvis en domstols dom eller beslut, som innebär att den åtalade frias från ansvar för brott, få genomslag även hos polisen på det sättet att en sådan person inte längre anges såsom misstänkt. Detsamma bör gälla när en förundersökning har lagts ned. Med detta avses dock inte att alla handlingar som rör brottsmisstanken måste rensas ut, utan enbart att den åtalade personen inte får utpekas såsom misstänkt och att man vid olika typer av sökningar inte ska få träff på honom eller henne i egenskap av misstänkt. Under den period uppgifterna i ärendet får behandlas i den brottsbekämpande verksamheten bör det däremot vid en sökning kunna vara möjligt att få fram en uppgift om att personen tidigare har varit misstänkt (se avsnitt 11.3). Detta gäller oavsett om beslut angående brottsmisstanken har meddelats av polisen eller av annan myndighet. Den föreslagna ordningen förutsätter att polisen följer upp avslutade ärenden.

Genom kravet på att det ska framgå att personen i fråga inte längre är misstänkt minskar risken för integritetsintrång. Härtill kommer att polisen sannolikt kommer att bevara flertalet av sina ärenden under viss tid efter att de har avslutats. Den fortsatta behandlingen har då inte sin grund i att det finns kvarstående misstankar mot personen i fråga utan i allmänna polisiära behov av att bevara avslutade ärenden.

Sammantaget väger polisens behov av att kunna ha tillgång till ärenden under viss tid efter att de har avslutats tyngre än det integritetsintrång som det kan innebära för en tidigare misstänkt person att uppgifter om honom eller henne förekommer i polisens datasystem.

Tillgång till avslutade förundersökningar

I det inledande avsnittet om bevarande och gallring redovisas polisens allmänna behov av att bevara uppgifter i ärenden en viss tid efter det att ärendet avslutades. Behovet av bevarande gäller i hög grad för avslutade brottsutredningar. Liksom för andra uppgifter som behandlas inom polisen bör det, utöver den föreslagna generella bestämmelsen om längsta tid för bevarande av uppgifter, dock gälla en yttersta gräns för tillgången till uppgifter i avslutade brottsutredningar som har gjorts gemensamt tillgängliga. I stället för gallringsbestämmelser bör det, som tidigare nämnts, gälla begränsningar i möjligheten att efter viss tid behandla uppgifterna i den brottsbekämpande verksamheten.

De skäl som redovisas i promemorian till stöd för polisens särskilda behov av att kunna fortsätta att behandla uppgifter i avslutade brottsutredningar är väl avvägda. Redovisningen överensstämmer i stort med de behov som *Rikspolisstyrelsen* redovisar i sitt remissvar. Polisen har exempelvis behov av uppgifterna för att lättare kunna utreda nya brott begångna av samma person eller mot samma person. Om en person återfaller i brott, har ofta tidigare brottsutredningar intresse. Vet man att det nya brottet har begåtts tillsammans med andra, okända gärningsmän, kan uppgifter om medgärningsmän i en tidigare brottsutredning vara av intresse. Vidare kan det tillvägagångssätt som användes vid det tidigare brottet ha betydelse. En äldre utredning kan också underlätta framtagandet av personutredning. Vid upprepade brott mot samma offer kan äldre utredningar utnyttjas bl.a. för att belysa förhållandet mellan förövare och offer och förekomsten av påtryckningar. Dessutom har polisen behov av att ta vara på information från brottsutredningar för att systematiskt samla information om vissa typer av brott eller vissa brottslingars beteenden. Sådan information har framför allt betydelse för det brottsförebyggande arbetet. Ett ytterligare behov är att kunna utnyttja tidigare brottsutredningar för utbildning och allmän kompetensutveckling inom polisen, eftersom både goda och dåliga exempel bör tas till vara.

När det gäller förundersökningar som har lagts ned, eller avslutats genom annat beslut som inte har lett till domstolsprövning (exempelvis beslut om förundersökningsbegränsning eller åtalsprövning), finns det också som promemorian pekar på ett annat verksamhetsbehov, nämligen behovet av att kunna återuppta brottsutredningen. Ett beslut om att inte driva en brottsutredning vidare kan ha många olika orsaker, av vilka en del i princip utesluter att utredningen kan komma att tas upp på nytt medan det i andra fall är mer eller mindre troligt att förundersökningen kan komma att återupptas. En förundersökning som har lagts ned eller inte lett till åtal på grund av att bevisningen har bedömts vara otillräcklig kan när som helst aktualiseras på nytt, om det kommer fram nya uppgifter. Likaså kan ett beslut att lägga ned en förundersökning, därför att det inte finns något uppslag om vem gärningsmannen är, snabbt bli inaktuellt om polisen får tips om gärningsmannen eller det kommer fram nya vittnesuppgifter eller annan bevisning. Vidare bör givetvis en förundersökning som har lagts ned för att den misstänkte har lämnat landet och inte kan förväntas återkomma kunna tas upp på nytt, om den misstänkte sedermera anträffas här i landet.

Det är mot den angivna bakgrunden rimligt att uppgifter i förundersökningar får vara tillgängliga i polisens brottsbekämpande verksamhet även en viss tid efter det att saken har avslutats. Denna tid bör dock inte vara alltför lång. Fem år utgör en rimlig avvägning mellan integritetsintressen och polisens verksamhetsbehov. Därför föreslås att personuppgifter i förundersökningar eller liknande brottsutredningar inte ska få behandlas i polisens brottsbekämpande verksamhet 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. Om polisen redan innan femårsgränsen har löpt ut bedömer att uppgifterna i ärendet inte längre behöver vara tillgängliga i den brottsbekämpande verksamheten får uppgifterna i ärendet inte bevaras där. Detta följer av den generella bestämmelsen om längsta tid för bevarande. Bland annat mot denna bakgrund får de av *Datainspektionen* åberopade kraven på bestämmelser om bevarande och gallring som ställs bl.a. i dataskyddskonventionen anses uppfyllda. Inspektionens invändning att de i promemorian föreslagna gallringsfristerna som anger längsta tid för bevarande inte är tillräckligt preciserade bemöts även i avsnitt 14.1.

I sammanhanget är det viktigt att påminna om att lagens övriga bestämmelser innebär att tillgången till uppgifter i förundersökningar kommer att begränsas på olika sätt. Tillgången till uppgifter ska t.ex. anpassas till tjänstemännens behov av uppgifterna. Alla uppgifter får inte heller vara sökbara.

Tillgång till förundersökningar även efter fem år

Uppgifter i avslutade förundersökningar får behandlas längre än fem år om uppgifterna behövs i en ny förundersökning eller för ett underrättelseprojekt som inletts före femårsfristens utgång. *Rikspolisstyrelsen* anser dock att polisen behöver ha tillgång till uppgifter i avslutade förundersökningar under längre tid än fem år även i andra fall. Styrelsen framhåller framförallt behovet av uppgifter i förundersökningar som lett till fällande domar och uppgifter i nedlagda förundersökningar där det aktuella brottet ännu inte preskriberats. I fråga om sistnämnda förundersökningar föreslås i promemorian att dessa bör få behandlas längre tid än fem år under förutsättning att förundersökningsledaren i samband med nedläggningsbeslutet har konstaterat att brottet trots beslutet kan komma att bli föremål för lagföring. Syftet med promemorians förslag var att, i förekommande fall, skapa utrymme för behandling fram till dess att brottet preskriberas. En sådan ordning är, som *Åklagarmyndigheten* påpekar, inte lämplig. Därför bör förslaget i den delen inte genomföras.

Som *Rikspolisstyrelsen* framhåller kan det finnas verksamhetsskäl som talar för att polisen ska kunna ha fortsatt tillgång till vissa uppgifter ur förundersökningar efter fem år. Av hänsyn till enskildas integritet finns det dock efter femårsfristen inte skäl att tillåta fortsatt behandling av hela förundersökningen i den brottsbekämpande verksamheten utan tillgången bör begränsas till vissa kategorier av uppgifter. Det skulle exempelvis sannolikt räcka att i en förundersökning som lett till fällande dom behandla uppgifter om den dömde, omständigheterna kring brottet och

ärendenummer eller liknande referensuppgift. Med hjälp av dessa uppgifter skulle ärendet kunna återfinnas i myndighetens arkiv (om handlingarna arkiverats). Motsvarande torde gälla beträffande nedlagda förundersökningar. Som *Rikspolisstyrelsen* konstaterar kan det också finnas skäl att ha tillgång till vissa uppgifter i brottsanmälningar och förundersökningar som avser brott där det är särskilt vanligt med återfall. Vidare kan det finnas skäl för fortsatt behandling av vissa andra kategorier av uppgifter, exempelvis vissa uppgifter om gods, uppgifter om efterlysta personer eller pornografiska skildringar av barn.

Föreskrifter om behandling av vissa kategorier av uppgifter i avslutade brottsutredningar under längre tid än fem år bör vara väl preciserade. De närmare ändamålen för behandlingen bör anges liksom när uppgifterna senast ska gallras. Bland annat med hänsyn till att sådana föreskrifter kommer att vara detaljerade och till att polisens behov kan komma att förändras över tiden bör föreskrifterna inte meddelas i lag utan i förordning. I avsnitt 14.1 föreslås att regeringen ska ha möjlighet att meddela föreskrifter om att vissa kategorier av uppgifter ska få behandlas längre än de i lagen angivna fristerna.

I promemorian föreslås bestämmelser i lag som begränsar möjligheten att efter femårsfristen använda uppgifter som arkiverats, bl.a. möjligheten att återföra arkiverat material till den brottsbekämpande verksamheten. Som tidigare anförts bör föreskrifter om behandlingen och tillgången till digitalt arkiverade uppgifter i stället meddelas av regeringen (se avsnitt 14.1).

Tillgång till brottsanmälningar som inte har lett till förundersökning

Anmälningar om brott är en typ av uppgifter som förtjänar särskild reglering. Ett stort antal brottsanmälningar leder till ett omedelbart beslut att inte inleda förundersökning. Skälet till detta är i flertalet fall att det saknas uppgifter om vem som kan misstänkas för brottet och att det inte heller i övrigt finns några uppgifter som kan bidra till utredningen om brottet. Som konstaterats i promemorian utesluter emellertid inte detta att brottsanmälan kan aktualiseras senare. Det kan komma fram nya omständigheter som kan leda till att brottet klaras upp, t.ex. om någon grips för likartade brott eller om gärningsmannen självmant erkänner brottet. Fram till den tidpunkt när brottet preskriberas finns det därför alltid ett latent behov av att kunna återuppta behandlingen av en brottsanmälan som inte har lett till förundersökning eller annan utredning. Bland annat mot den bakgrunden bör en brottsanmälan få vara tillgänglig i polisens brottsbekämpande verksamhet även efter det att ärendet avslutats. Uppgifterna bör dock aldrig få behandlas i den brottsbekämpande verksamheten efter det att det brott som anmälan avser har preskriberats. En särskild bestämmelse om detta bör införas i den nya lagen.

Vad som nu har sagts bör dock inte gälla för de brottsanmälningar som har avskrivits på den grunden att det inte har förekommit något brott. Sådana anmälningar bör enligt huvudregeln inte kunna behandlas längre än vad som behövs för handläggningen. Som exempel kan bl.a. nämnas vad som brukar kallas okynnesanmälningar (som oftast sker i syfte att trakassera eller svärta ned den anmälde) och anmälningar som bygger på

bristande verklighetsuppfattning (t.ex. på grund av sjukdom hos anmälaren). Det skulle strida mot de allmänna principerna för behandling av personuppgifter i polisens verksamhet att tillåta en längre tids behandling av brottsanmälningar som avser beteenden som inte utgör något brott i juridisk mening. Som *Åklagarmyndigheten* framhåller bör undantaget dock inte omfatta grundlösa anmälningar i allmänhet utan, som promemorian föreslagit, endast sådana anmälningar som avser ett handlande som, enligt behörig beslutsfattare, över huvud taget inte utgör något brott.

15 Särskilda bestämmelser om vissa register

15.1 Allmänna utgångspunkter

Regeringens förslag: I den nya lagen införs särskilda bestämmelser om register över DNA-profiler, fingeravtrycks- eller signalementsregister, penningtvättsregister och ett internationellt register.

Utredningens förslag överensstämmer delvis med promemorians. Utredningen har dock föreslagit att även det allmänna spaningsregistret ska regleras särskilt i den nya lagen. Utredningen föreslår inte någon särreglering av penningtvättsregister eller det internationella registret.

Remissinstanserna: De flesta remissinstanser har inte haft någon invändning mot utredningens förslag. *Datainspektionen* har ansett att även Rationell anmälningsrutin (RAR) bör författningsregleras. *Sveriges advokatsamfund* har ansett att särskilda regler bör övervägas beträffande ändamål, innehåll och gallring när det gäller det digitala referensbiblioteket över barnpornografiska framställningar.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås dock inget särskilt register för behandlingen av internationella ärenden.

Remissinstanserna: Flertalet remissinstanser ställer sig bakom eller har inget att invända mot promemorians förslag. *Riksdagens ombudsmän* anser dock att registerbegreppet bör reserveras för manuellt förda register och över huvudtaget inte användas i den nya lagstiftningen. *Rikspolisstyrelsen* anser att även IT-systemet ”Digitalt referensbibliotek över barnpornografiska framställningar” bör regleras särskilt. Styrelsen framhåller vidare att den behandling som sker i det internationella dokument- och ärendehanteringssystemet benämnt DAR II inte kommer att kunna fortsätta att ske på ett ändamålsenligt sätt om förslaget genomförs.

Skälen för regeringens förslag: Såväl Polisdatautredningen som promemorian innehåller förslag om särbestämmelser för några av polisens nuvarande register, trots att utgångspunkten har varit att åstadkomma en generell reglering.

Målsättningen bör vara att i möjligaste mån undvika särreglering av vissa speciella informationssamlingar eller viss personuppgiftsbehandling. Det huvudsakliga skälet för detta är, som utvecklas närmare i avsnitt 6.1, att den nya regleringen så långt som möjligt bör vara teknikneutral.

Genom att utforma den nya lagen som en rättslig ram för vilka uppgifter som får behandlas och på vilket sätt uppgifterna får användas blir det möjligt för polisen att bygga upp datasystem som bättre tillgodoser både intresset av att mer effektivt utnyttja tillgänglig information och intresset av att skydda enskildas personliga integritet. Inom den brottsbekämpande verksamheten finns det emellertid viss behandling av personuppgifter som av olika skäl inte bör inordnas under de generella bestämmelserna. Det är därför enligt regeringens mening nödvändigt att i några fall ha särskilda bestämmelser om vissa register, vilket även Polisdatautredningen och promemorian förespråkar. Dessa bestämmelser bör tillämpas på behandlingen av uppgifter i respektive register och gälla i stället för de särskilda bestämmelser som föreslås gälla för gemensamt tillgängliga uppgifter. Det finns, på samma sätt som nu, skäl att ha särskilda bestämmelser om dels register över DNA-profiler, dels fingeravtrycks- eller signalementsregister. Detsamma bör, som anges i promemorian, gälla för behandling av uppgifter om misstänkt penningtvätt och misstänkt finansiering av terrorism i penningtvättsregister. Vidare finns det enligt regeringens mening skäl att särreglera viss behandling av uppgifter i det internationella polissamarbetet. Därför föreslås bestämmelser om ett internationellt register. Skälen för en särreglering varierar och redovisas därför för varje register för sig (avsnitt 15.2–5). Även det allmänna spaningsregistret bör regleras särskilt. Detta register bör dock, som föreslås i promemorian, regleras i en särskild lag (avsnitt 19).

Riksdagens ombudsmän anför att begreppet register bör reserveras för manuellt förda register. I och med att de system som föreslås bli särreglerade är avgränsade uppgiftssamlingar och att flertalet av dem redan benämns register bör denna benämning användas även fortsättningsvis. Det kan anmärkas att det är relativt vanligt att begreppet register används för automatiserade uppgiftssamlingar. Detta gäller även för nyinrättade sådana, se t.ex. den nyligen beslutade lagen (2009:619) om djurskyddskontrollregister.

Rikspolisstyrelsen föreslår att även IT-systemet ”Digitalt referensbibliotek över barnpornografiska framställningar” bör regleras särskilt. Huvudskälet är att barnpornografiska framställningar behöver bevaras under längre tid än vad de föreslagna gallringsbestämmelserna tillåter. Med hänsyn till målsättningen att undvika särregleringar av register, bör det, enligt regeringens mening, i stället för en särreglering meddelas föreskrifter på förordningsnivå om undantag från lagens bestämmelser om gallring och om längsta tid för bevarande. I avsnitt 14.1 föreslås att regeringen ska ha möjlighet att meddela sådana föreskrifter.

På motsvarande sätt bör frågan om att bevara uppgifter som behandlas i det centrala brottsspaningsregistret kunna lösas. Någon särreglering av det registret behövs därför inte heller. I promemorian övervägs frågan och samma bedömning görs där. Det centrala brottsspaningsregistret bildar ett särskilt register över anmälda allvarligare brott och är avsett att kunna utnyttjas för såväl spaning som brottsutredning. I registret behandlas bl.a. uppgifter om tillvägagångssätt vid brott (modus operandi). Som konstateras i promemorian kommer de uppgifter som behandlas i det centrala brottsspaningsregistret i allt väsentligt att kunna behandlas även i fortsättningen, dock inte under lika lång tid. Tidigare har gjorts bedömningen att polisen, med stöd av bestämmelser på förordningsnivå,

bör tillåtas att bevara vissa kategorier av uppgifter, bl.a. uppgifter ur avslutade förundersökningar, under längre tid än den i lagen föreslagna femårsfristen (se avsnitt 14.1 och 14.4). Om det skulle visa sig att det finns ett behov av att bevara visst slag av uppgifter som för närvarande behandlas i det centrala brottsspaningsregistret under längre tid än de i lagen föreslagna fristerna, har regeringen således möjlighet att meddela föreskrifter om detta.

I avsnitt 12 behandlas frågor om direktåtkomst och i avsnitt 13 frågor som rör sekretess, däribland sekretessen för uppgifterna i särskilda register.

15.2 Register över DNA-profiler

Regeringens förslag: Rikspolisstyrelsen får behandla DNA-profiler i särskilda register dels för brottsbekämpande ändamål, dels för att underlätta identifiering av avlidna personer i andra fall.

Gallring i registren ska i huvudsak regleras på samma sätt som nu.

Utredningens förslag överensstämmer i huvudsak med promemorians. Sedan utredningen lämnade sitt förslag har dock bestämmelserna om register över DNA-profiler varit föremål för behandling i ett annat lagstiftningsärende (se prop. 2005/06:29) och nya bestämmelser har trätt i kraft (SFS 2005:877).

Remissinstanserna: Flertalet remissinstanser har inte haft någon invändning mot utredningens förslag. *Riksarkivet* har föreslagit att det ska införas en möjlighet att föreskriva om undantag från gallring för historiska, vetenskapliga och statistiska ändamål.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inget att invända mot förslaget. *Statens kriminaltekniska laboratorium* uppger att brottskod och misstankenummer för närvarande registreras i DNA-registren och anser att sådana uppgifter behöver kunna registreras även fortsättningsvis. Vidare föreslår myndigheten att uppgift om kön bör få registreras. Laboratoriet stödjer förslaget att registren bör få användas i syfte att identifiera avlidna personer och väcker frågan om inte registren även skulle kunna användas för att underlätta identifiering av levande personer som inte kan identifieras på något annat sätt. Enligt laboratoriet kan det också vara lämpligt att i lagtexten använda en mindre kategorisk skrivning vad gäller förbudet mot att registrera analysresultat som kan ge upplysningar om personliga egenskaper. Den del av DNA som typbestäms hör till den icke kodande delen av DNA:t, dvs. inga personliga egenskaper är kopplade till dessa. Enligt laboratoriet går det dock antagligen inte att helt utesluta att man i framtiden upptäcker att någon av dessa ändå är kopplad till en gen som t.ex. kan ge en viss sjukdom. *Riksarkivet* föreslår att det ska införas en möjlighet att föreskriva om undantag från gallring för historiska, vetenskapliga och statistiska ändamål.

Skälen för regeringens förslag: Nya bestämmelser om användningen av DNA-tekniken inom brottsbekämpningen trädde i kraft den 1 januari 2006 (prop. 2005/06:29, bet. 2005/06:JuU7, rskr. 2005/06:58). Bestäm-

melserna har tillämpats i nästan fyra år och har visat sig vara ändamålsenliga. Det har inte framkommit något som ger anledning att i detta sammanhang göra några mera omfattande ändringar i polisdatalagens reglering av register över DNA-profiler. Att registren särregleras motiveras av att det är ett speciellt slag av uppgifter som behandlas. Det kan även anmärkas att Prümrådsbeslutet (se nedan) förutsätter att varje medlemsstat har nationella register över DNA-profiler. De aktuella bestämmelserna i polisdatalagen bör därför i allt väsentligt oförändrade föras över till den nya lagen. Vissa redaktionella och språkliga ändringar bör dock göras. I avsnitt 9.6 föreslås att begreppet DNA-profil införs. Vidare redogörs för vilka begränsningar som bör gälla för behandlingen av DNA-profiler utanför de register som regleras särskilt.

Det internationella polissamarbetet och informationsutbytet utvecklas snabbt, särskilt inom EU. Prümrådsbeslutet är ett exempel på detta. Av Prümrådsbeslutet följer bl.a. att medlemsstaterna ska ge varandra direktåtkomst till uppgift om huruvida någon förekommer i DNA-register och att automatiska jämförelser av oidentifierade DNA-profiler ska kunna göras. För att möjliggöra detta måste den nya lagen ge utrymme för sådan behandling. Mycket talar för en fortsatt utveckling av informationsutbytet med andra stater, särskilt inom EU. Den nya lagen bör därför möjliggöra inte bara sådan behandling som krävs enligt nu ingångna överenskommelser utan regleringen bör utformas generellt. En särskild bestämmelse bör införas som tillåter jämförelser av DNA-profiler i spårregistret om det är nödvändigt för att fullgöra en internationell överenskommelse som riksdagen har godkänt. Detsamma bör gälla om en sådan skyldighet följer av en EU-rättsakt. Möjligheten att bevilja utländska myndigheter direktåtkomst behandlas i avsnitt 12.3.5. I departementspromemorian Genomförande av delar av Prümrådsbeslutet (Ds 2009:8) har motsvarande bestämmelser föreslagits i polisdatalagen.

I en lagrådsremiss den 8 oktober 2009 har regeringen föreslagit att åtalspreskription, påföljdspreskription och absolut preskription ska avskaffas för vissa brott, om dessa har begåtts av vuxna lagöverträdare. De brott som avses är mord, dråp, grovt folkrättsbrott, folkmord samt terroristbrott som begåtts genom mord eller dråp. Även försök till sådana brott, med undantag för grovt folkrättsbrott, ska enligt förslaget undantas från preskription. Vidare har föreslagits att sådana uppgifter i det spårregister som innehåller DNA-profiler som hänför sig till nyssnämnda brottstyper ska gallras senast sjuttio år efter registreringen, i stället för trettio år. Ändringarna föreslås träda i kraft den 1 juli 2010. Motsvarande reglering bör införas i den nya lagen.

Frågan är om det bör göras några ytterligare ändringar i regleringen av register över DNA-profiler. Som föreslås i promemorian bör DNA-registren få användas för identifiering av avlidna personer även om behandlingen inte sker för något brottsbekämpande ändamål. *Statens kriminaltekniska laboratorium* väcker frågan om inte registren också bör få användas för annat än brottsbekämpande ändamål i syfte att identifiera okända personer som är i livet. Detta skulle kunna innebära en betydande utvidgning av användningen av registren. En sådan förändring bör inte genomföras utan att frågan utreds närmare. Detsamma gäller den av laboratoriet väckta frågan om huruvida uppgift om en persons kön bör få

registreras i register över DNA-profiler. Frågorna bör därför inte behandlas inom ramen för detta lagstiftningsärende.

Brottskod och misstankenummer bör, som *Statens kriminaltekniska laboratorium* påpekar, även fortsättningsvis få registreras i register över DNA-profiler. Dessa uppgifter får anses inrymmas i ”upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser” (24–25 §§ polisdatalagen). I förtydligande syfte bör det dock i den nya lagen uttryckligen anges att brottskod får registreras. Detta överensstämmer också med vad som föreslås beträffande fingeravtrycks- eller signalementsregister i avsnitt 15.3.

Det är av central betydelse, inte minst ur integritetssynpunkt, att registreringen av en DNA-profil endast ger information om den registrerades identitet. Det är inte tillåtet att registrera uppgifter om personliga egenskaper. Att det inte går att utesluta att det någon gång i framtiden skulle kunna gå att utvinna viss ytterligare information ur de DNA-profiler som registreras bör inte föranleda någon ändring av gällande lagstiftning. Det är dock viktigt att utvecklingen och användningen av DNA-tekniken noga följs och fortlöpande utvärderas i syfte att uppmärksamma eventuella framtida behov av lagändringar.

Riksarkivet vidhåller sin tidigare framförda uppfattning att det bör införas en möjlighet att föreskriva om undantag från gallring av uppgifter i DNA-registren om det behövs för historiska, vetenskapliga och statistiska ändamål. Myndigheten framhåller att den ökande betydelsen av DNA-tekniken kan innebära att det blir ytterst värdefullt för någon om dagens uppgifter i dessa register sparas. Enligt myndigheten bör det i vart fall vara av stort värde att sådana uppgifter sparas som referensmaterial för historiska, vetenskapliga och statistiska ändamål. Varken Polisdatautredningen eller promemorian föreslår någon sådan möjlighet. I promemorian görs bedömningen att intresset av att bevara uppgifterna för angivna ändamål inte kan anses uppväga det intresse som motiverar gallringsbestämmelserna, nämligen skyddet för den enskildes personliga integritet. Det har inte framkommit skäl att göra någon annan bedömning. Det bör därför inte införas någon möjlighet att föreskriva om undantag från gallringsbestämmelserna för registren över DNA-profiler.

I 27 a § polisdatalagen finns en särskild gallringsregel för DNA-prov. Prümrådsbeslutet ställer krav på att sådana prov ska kunna tas på en annan stats begäran. Det aktualiserar ett tillägg i gallringsregeln. I promemorian som behandlar genomförandet av Prümrådsbeslutet har föreslagits en särskild gallringsfrist för sådana prov. Av praktiska skäl bör det gälla en enhetlig gallringsfrist för de prov som tas för DNA-analys. Den bör, som är huvudregeln enligt gällande rätt, vara sex månader.

I avsnitt 12.3 och 12.4 behandlas frågorna om direktåtkomst till registren och möjligheten att lämna ut uppgifter ur registren på medium för automatiserad behandling. I avsnitt 13 behandlas frågor om sekretess.

15.3 Fingeravtrycks- eller signalementsregister

Regeringens förslag: Rikspolisstyrelsen får behandla uppgifter om fingeravtryck, fotografier, signalement och videoupptagningar i särskilda fingeravtrycks- eller signalementsregister för brottsbekämpande ändamål och för att underlätta identifiering av okända personer även i andra fall.

Särskilda gallringsbestämmelser ska gälla för uppgifter i sådana register. Om fingeravtryck har tagits av en person på grund av misstanke om brott, får uppgifter om personen finnas kvar i fingeravtrycks- eller signalementsregister så länge det finns uppgifter om honom eller henne i misstankeregistret eller belastningsregistret. Uppgifterna i fingeravtrycks- eller signalementsregister ska gallras senast tre månader efter det att uppgifterna om personen har gallrats ur belastningsregistret och misstankeregistret. Uppgifter om fingeravtryck som har kommit fram under utredning av brott och som hänför sig till oidentifierade personer (spår) ska enligt huvudregeln gallras senast trettio år efter registreringen och i vissa fall senast efter sjuttio år.

Regeringen eller den myndighet som regeringen bestämmer har, trots gallringsbestämmelserna, möjlighet att meddela föreskrifter om att uppgifter får bevaras under längre tid för historiska, statistiska eller vetenskapliga ändamål.

Utredningens förslag överensstämmer delvis med promemorians. Utredningen föreslår en annan gallringsregel.

Remissinstanserna: Flertalet remissinstanser har inte haft någon invändning mot utredningens förslag. *Riksarkivet* har föreslagit att det införs en möjlighet att föreskriva om undantag från kravet på gallring.

Promemorians förslag överensstämmer delvis med regeringens. I promemorian föreslås inga särskilda bestämmelser om behandling av uppgifter för att fullgöra internationella åtaganden eller behandling av oidentifierade spår. Det föreslås inte heller någon definition av fingeravtryck, eller att fotografier eller videoupptagningar får registreras. Promemorian föreslår en annan utformning av gallringsreglerna, som knyter an till brottens svårhetsgrad. Promemorian föreslår ingen bestämmelse som ger stöd för att meddela föreskrifter om undantag från gallringsbestämmelserna för historiska, statistiska eller vetenskapliga ändamål.

Remissinstanserna: *Rikspolisstyrelsen* är den enda remissinstans som framför invändningar mot promemorians förslag. Styrelsen anser att fingeravtrycks- eller signalementsregistren bör få innehålla uppgifter i digital form av friktionshudsupptagning av fot, handflata och fingeravtryck, fotografier, rörliga bilder samt ljud.

Styrelsen anser vidare att det bör införas särskilda gallringsbestämmelser för uppgifter som registreras inom ramen för det internationella samarbetet, för uppgifter om försvunna personer och för uppgifter om personer som utvisats ur Sverige. Rikspolisstyrelsen anser också att den tid under vilken en person avtjänar t.ex. ett fängelsestraff inte ska räknas med vid beräkningen av de föreslagna gallringsfristerna.

Enligt Rikspolisstyrelsen bör fingeravtrycks- och signalementsuppgifter få bevaras även efter att en förundersökning har avslutats. Sådana

uppgifter bevaras inte i förundersökningen. Skulle en förundersökning återupptas är det viktigt att kunna verifiera ett sakkunnigutlåtande, exempelvis om att ett avtryck funnits på visst föremål, genom att kontrollera grundhandlingen som utlåtandet bygger på. Ett annat skäl mot att gallra uppgifterna är att stöldgods med fingeravtryck kan komma fram efter att en förundersökning lagts ned. Om den misstänktes fingeravtryck har gallrats försvåras möjligheten att klara upp brottet. Styrelsen menar att det finns ett berättigat polisiärt intresse att fortsätta att behandla uppgifter om en misstänkt i de fall där förundersökningen läggs ned på grund av bristande bevisning. Styrelsen gör bedömningen att en majoritet av förundersökningar som har lagts ned efter det att en person daktyloskoperats kan komma att återupptas om ny bevisning framkommer.

Rikspolisstyrelsen anser vidare att Riksarkivet bör ges möjlighet att meddela föreskrifter om undantag från gallring. Styrelsen framhåller att det inom ramen för pågående forskning för metodutveckling angående fingeravtryck är viktigt att över tiden kunna jämföra resultat från olika identifieringsmetoder med t.ex. sakkunnigutlåtanden. Möjligheten till sådan forskning kan enligt styrelsen förloras om det inte finns möjlighet bevara fingeravtryck för vetenskapliga ändamål.

Skälen för regeringens förslag

Gällande bestämmelser och allmänna utgångspunkter

I 29–31 §§ polisdatalagen finns bestämmelser om fingeravtrycks- och signalementsregister. Rikspolisstyrelsen får behandla uppgifter i sådana register för att underlätta identifiering av personer i samband med brott. Uppgifterna får vidare användas för identifiering av okända personer i andra fall. Sådana uppgifter får också behandlas i förundersökningar och särskilda undersökningar (29 §). I 30 § regleras under vilka förutsättningar som uppgifter får föras in i registren och vad registren får innehålla. Där sägs bl.a. att sådana register får innehålla endast uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck med stöd av en viss bestämmelse i lagen om särskild utlänningskontroll. Registren får inte innehålla fingeravtryck som med stöd av lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare tagits av den som är under femton år. I registren får det endast antecknas uppgifter om fingeravtryck, signalement, identifieringsuppgifter och ärendenummer.

Bestämmelserna i 29–31 §§ polisdatalagen har dock i praktiken inte tillämpats. Rikspolisstyrelsen för i stället ett fingeravtrycksregister och ett signalements- och känneteckensregister med stöd av den upphävda datalagen och tillstånd från Datainspektionen enligt övergångsbestämmelserna till polisdatalagen (se *bilaga 6*). Det innebär att polisdatalagens bestämmelser inte gäller för registren. Polisdatalagens bestämmelser överensstämmer emellertid i stort med de föreskrifter som Datainspektionen har meddelat för registren. Gallringsbestämmelserna för signalements- och känneteckensregistret är dock något annorlunda utformade.

Som Polisdatautredningen och promemorian föreslår bör fingeravtrycks- och signalementsregister regleras särskilt. En särreglering av fingeravtrycksregistret motiveras framförallt av att det rör sig om ett

speciellt slag av uppgifter som kräver en särskilt teknisk lösning för att kunna behandlas. Det kan även noteras att Prümrådsbeslutet förutsätter att varje medlemsstat har ett nationellt fingeravtrycksregister. En särreglering av signalementsregister behövs för att särskilja behandlingen av de uppgifter som lämnas till Rikspolisstyrelsen med stöd av förordningen (1992:824) om fingeravtryck m.m. (fingeravtrycksförordningen) från behandlingen av andra liknande uppgifter. Vid utformningen av de nya reglerna om fingeravtrycks- och signalementsregister bör bestämmelserna om registren i polisdatalagen bilda utgångspunkt.

Regleringen bör dock, som föreslås i promemorian, anpassas till den nya utformningen av polisens personuppgiftsbehandling i övrigt. De personuppgifter som får förekomma i fingeravtrycksregister och signalementsregister kan inte anses vara så känsliga att man behöver begränsa behandlingen av uppgifterna till enbart förundersökningar och särskilda undersökningar. Sådana uppgifter bör således få behandlas i polisens brottsbekämpande verksamhet i dess helhet. Den reglering som nu föreslås bör gälla enbart behandlingen i de särskilda fingeravtrycks- eller signalementsregister som främst bygger på uppgifter som sänds till Rikspolisstyrelsen enligt fingeravtrycksförordningen, vilket utvecklas närmare nedan. Behandling i registren bör, som föreslås i promemorian, få ske för brottsbekämpande ändamål och för att underlätta identifiering av okända personer även i andra fall.

Innehållet i registren

Enligt 28 kap. 14 § rättegångsbalken och fingeravtrycksförordningen ska fingeravtryck och fotografi alltid tas av den som häktats som misstänkt för brott. I vissa uppräknade fall ska fingeravtryck och fotografi också tas av den som är anhållen och under vissa förutsättningar får sådana åtgärder även vidtas beträffande annan som är misstänkt för brott. Misstänkta får även videofilmas och av sådan person får även tas avtryck av hand, fot eller öra. Fingeravtryck, fotografi samt avtryck av hand eller fot ska enligt 7 § fingeravtrycksförordningen skyndsamt sändas till Rikspolisstyrelsen tillsammans med en beskrivning av personen. Rikspolisstyrelsen har med stöd av förordningen meddelat föreskrifter och allmänna råd om fingeravtryck och signalementsupptagning (RPSFS 2005:12; FAP 473–1).

I Rikspolisstyrelsens fingeravtrycksregister och signalements- och känneteckensregister registreras flertalet av de uppgifter som översänds med stöd av fingeravtrycksförordningen. I fingeravtrycksregistret registreras också uppgifter om fingeravtryck som tas enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I registret finns även fingeravtrycksuppgifter som översänts inom ramen för det internationella samarbetet, t.ex. avseende personer som är efterlysta av Interpol. Vidare innehåller registret fingeravtryck som har kommit fram vid utredning av brott och som inte kan hänföras till någon identifierbar person (spår). När ett fingeravtryck från en brottsplats jämförts med fingeravtrycken i registret utan att avtrycket kunnat identifieras registreras spåret i syfte att senare kunna identifiera den person som avsatt avtrycket.

Rikspolisstyrelsens fingeravtrycks- och signalementsregister bör även fortsättningsvis i huvudsak bygga på sådana uppgifter som rapporteras till styrelsen enligt fingeravtrycksförordningen. Detta bör tydliggöras i lagtexten i syfte att särskilja dessa register från annan behandling med stöd av lagen, exempelvis behandling av signalementsuppgifter i en förundersökning eller i ett underrättelseprojekt. Det bör i lagen även tydligt framgå att det är tillåtet att behandla oidentifierade fingeravtryck (spår) i registren. Dessutom bör det särskilt anges att det är tillåtet att behandla uppgifter i enlighet med internationella åtaganden. Här rör det sig framför allt om behandling av fingeravtryck som översänds från andra stater för att jämföras med uppgifter i svenska register. Behovet av att registrera fingeravtryck nationellt inom ramen för det internationella samarbetet kommer att minska genom Prümsamarbetet, eftersom fingeravtryck som har registrerats i en annan stat som deltar i samarbetet görs tillgängliga genom automatisk sökning i den andra statens fingeravtrycksregister.

Det bör liksom i gällande reglering anges vilka kategorier av uppgifter som får antecknas i registren. Fingeravtryck bör självfallet registreras. Handavtryck registreras för närvarande i fingeravtrycksregistret och bör få fortsätta att registreras. Det bör införas en definition i lagen som tydliggör att med fingeravtryck avses både avtryck av fingrar och hand. Motsvarande definition finns i artikel 2 i Rådets beslut 2008/616/RIF av den 23 juni 2008 om genomförande av Prümrådsbeslutet.

Rikspolisstyrelsen anser att fingeravtrycks- och signalementsregistren även bör få innehålla fotavtryck, fotografier, rörliga bilder samt ljud. Fotografier lagras för närvarande i ett manuellt register. Till detta register finns hänvisningar i fingeravtrycks- och signalementsregistren genom att fotonummer anges. Att inte fotografier omnämns i Datainspektionens tillstånd (där anges endast fotonummer) eller i polisdatalagen torde framförallt bero på att det tidigare inte fanns tekniska möjligheter att lagra fotografier digitalt. Det finns inte heller tekniskt stöd i nuvarande datasystem för sådan registrering.

Om fotografier tillåts behandlas digitalt i registren, i stället för i manuella kartotek, ökar tillgängligheten till fotografierna. Polisen har ett intresse av att snabbt kunna få tillgång till fotografier av misstänkta. Fotografier kan behövas både för att identifiera en viss person som är misstänkt och för att avföra personer från vidare misstanke. För närvarande måste en tjänsteman kontakta Nationella fingeravtrycksavdelningen vid Rikskriminalpolisen inom Rikspolisstyrelsen, som handhar de aktuella registren, och begära ut en papperskopia av efterfrågat fotografi. Denna hantering framstår som ineffektiv, tidsödande och otidsenlig. Fotografier bör därför kunna lagras digitalt.

Fingeravtrycks- eller signalementsregister bör även få innehålla videoupptagningar. Det kan finnas skäl för polisen att ha tillgång till dokumentation av en persons rörelsemönster eller liknande som har gjorts med stöd av 28 kap. 14 § rättegångsbalken och bestämmelser i fingeravtrycksförordningen. Sådana videoupptagningar kan naturligtvis innehålla både ljud och bild. I och med att ljudupptagningar inte regleras särskilt i nämnda bestämmelser bör detta inte heller göras i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det saknas för närvarande skäl att införa en möjlighet att kunna registrera

fotavtryck, eftersom något behov av en sådan registrering inte har kommit fram.

Även brottskoder bör få registreras i fingeravtrycks- eller signalementsregister. Det finns framförallt ett behov av att anteckna sådana uppgifter i signalementsregistret. Användningen av enbart uppgifter om signalement och andra kännetecken ger normalt ett alldeles för stort antal träffar i registret för att en sökning ska vara effektiv. Genom att använda brottskoder vid sökningen kan man begränsa sökresultatet. Användandet av brottskoder innebär, som konstateras i promemorian, knappast heller några ytterligare risker för den enskildes personliga integritet. Tvärtom får det till följd att antalet träffar vid en sökning begränsas, något som är positivt från integritetsskyddssynpunkt. Den nya lagen bör därför medge att brottskoder antecknas i de aktuella registren.

Gallring

Enligt 31 § polisdatalagen ska uppgifter i fingeravtrycks- och signalementsregister om en misstänkt person gallras när förundersökning eller åtal mot personen läggs ned eller när åtal ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den misstänkte ska behandlas med stöd av polisdatalagens bestämmelser om behandling av kvarstående misstankar. Om den registrerade döms, ska uppgifterna gallras senast när uppgifterna om personen gallras ur belastningsregistret.

I december 2005 meddelade Datainspektionen föreskrifter för fingeravtrycksregistret som överensstämmer med polisdatalagens gallringsbestämmelser. I juni 2006 och oktober 2008 meddelade myndigheten gallringsföreskrifter för signalements- och kännetecknsregistret. Föreskrifterna bygger på ett förslag som Rikspolisstyrelsen lämnade i ärendet och tar sin utgångspunkt i brottets svårhetsgrad. Ett brott av lindrigare karaktär innebär att uppgifterna får behandlas under betydligt kortare tid än om det är fråga om ett allvarligt brott.

I promemorian föreslås att gallringsbestämmelserna ska utformas efter sistnämnda modell. Förslaget innebär att uppgifterna ska gallras efter tio, femton eller tjugofem år. Vidare föreslås att den tid under vilken en person avtjänar t.ex. ett fängelsestraff inte ska räknas med vid beräkningen av gallringsfristerna. Enligt promemorian bör de angivna gallringsfristerna inte gälla när åtal mot den misstänkte har lagts ned eller när han eller hon har frikänts genom lagakraftvunnen dom. I sådana fall bör uppgifterna få sparas endast under tre månader. Detsamma föreslås gälla när förundersökningen mot en misstänkt har lagts ned.

Rikspolisstyrelsen anser att verksamhetsskäl talar för att fingeravtryck och signalement som härrör från förundersökningar som har lagts ned på grund av bristande bevisning bör få bevaras under längre tid. Hänsynen till enskildas integritet väger emellertid enligt regeringens mening tyngre än de verksamhetsskäl som Rikspolisstyrelsen framför. Fingeravtrycks- eller signalementsregister bör varken innehålla uppgifter om personer som har frikänts eller uppgifter om personer som inte längre är misstänkta i en förundersökning. Det är i sammanhanget viktigt att framhålla att gallringsbestämmelserna endast gäller uppgifterna i de aktuella registren. Bestämmelserna hindrar således inte att vissa uppgifter bevaras i

förundersökningen som en dokumentation av innehållet i ärendet. Från integritetssynpunkt är det stor skillnad mellan detta och att tillåta bevarandet av uppgifter om icke-misstänkta i ett register över misstänkta och dömda personer. Efter klagomål från två enskilda konstaterade Europadomstolen den 4 december 2008 i en dom att fortsatt bevarande av klagandenas DNA-prov, DNA-profiler och fingeravtryck efter frikännande dom respektive nedlagd förundersökning utgjorde en kränkning av artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (S. och Marper mot Storbritannien). I domen framhålls bl.a. betydelsen av att frikända personer ska behandlas som oskyldiga (s. 34). Det kan tillfogas att för den händelse en nedlagd förundersökning tas upp på nytt och senare resulterar i åtal och fällande dom det i regel finns grund för att åter registrera den misstänktes fingeravtryck.

Frågan är då hur gallringsregeln bör utformas. Den lösning som föreslås i promemorian innebär att gallring ska ske efter i princip samma riktlinjer som tillämpas vid gallring i belastningsregistret, nämligen i förhållande till brottets svårhetsgrad. Med den utgångspunkten är det enligt regeringens mening en bättre lösning att koppla gallringsfristerna direkt till att det förekommer uppgifter i belastningsregistret om personen i fråga, vilket Polisdatautredningen föreslår. Eftersom fingeravtryck normalt tillförs fingeravtrycksregistret redan när det finns en misstanke om brott måste en motsvarande koppling göras till misstankeregistret. Utgångspunkten bör alltså vara att så länge det finns uppgifter om personen i antingen belastningsregistret eller misstankeregistret får uppgifterna i fingeravtrycksregistret finnas kvar. Denna lösning motsvarar i sak vad som föreslås för gallring i register över DNA-profiler. Med denna lösning behövs ingen bestämmelse om att den tid under vilken personen verkställer påföljd inte ska räknas in i gallringsfristen. Bestämmelsen om gallring bör utformas på det sättet att uppgifter i fingeravtrycksregister ska gallras senast tre månader efter det att misstankeregistret och belastningsregistret har gallrats så att det inte längre finns några uppgifter om personen.

Rikspolisstyrelsen anser vidare att uppgifter om personer som utvisats på grund av brott ska få bevaras i registren under den tid förbudet att återvända till Sverige består. Med hänsyn till de relativt långa gallringsfrister som föreslås för registren kommer uppgifter om personer som utvisats för brott många gånger att bevaras under hela den tid som förbudet att återvända till Sverige består eller i vart fall under en stor del av denna tid. En sådan bestämmelse som Rikspolisstyrelsen föreslår skulle i vissa fall leda till att uppgifter om personer som utvisats skulle bevaras betydligt längre än uppgifter om andra dömda personer. Uppgifter om en person som utvisas på livstid skulle kunna bevaras så länge personen lever. Att bevaka hur länge utvisade personer lever torde för det första medföra praktiska svårigheter för polisen. För det andra kan det ifrågasättas om intresset av att säkerställa att beslutet inte överträds uppväger det integritetsintrång som det innebär för personen att hans uppgifter bevaras. I bedömningen måste även vägas in om efterlevnaden av återreseförbudet kan säkerställas på något annat sätt. I sammanhanget är det värt att notera att uppgifter om att en person ska nekas tillträde till Schengenområdet registreras i Schengens informationssystem. Mot den

bakgrunden bör den av Rikspolisstyrelsen förslagna förändringen inte genomföras utan att frågan utreds närmare, vilket inte är möjligt inom ramen för detta lagstiftningsärende.

Som Rikspolisstyrelsen föreslår bör det införas en särskild gallringsbestämmelse för uppgifter som registreras inom ramen för det internationella samarbetet. Det är lämpligt att gallringsfristen knyts till ändamålet med behandlingen. Om en person har efterlysts av Interpol, bör uppgifterna exempelvis gallras när personen i fråga har påträffats. Någon särskild gallringsfrist för försvunna personer bör dock inte införas, eftersom sådan behandling bara kan förekomma inom ramen för det internationella samarbetet och därmed omfattas av nyssnämnda gallringsbestämmelse.

Varken Polisdatautredningen eller promemorian berör frågan om behandling av fingeravtryck från oidentifierade personer, dvs. spår från brottsplatser. Regeringen föreslår att behandlingen av sådana fingeravtryck uttryckligen regleras i den nya lagen efter mönster av vad som gäller för oidentifierade DNA-spår. Gallringen av oidentifierade fingeravtryck bör göras efter samma principer som gäller för gallring av oidentifierade DNA-spår. Det innebär att fingeravtryck från oidentifierade personer enligt huvudregeln bör gallras senast trettio år efter registreringen.

Som tidigare nämnts föreslår regeringen i en lagrådsremiss att vissa brott ska undantas från preskription och i samband härmed föreslås ändrade gallringsregler för spårregistret med DNA-profiler. Det finns enligt regeringens mening ett motsvarande behov av att kunna bevara sådana fingeravtryck som har tagits fram under en utredning av ett brott som undantas från preskription och som inte hänför sig till en identifierbar person. De brott som avses är mord, dråp, folkmord, terroristbrott som begåtts genom mord eller dråp och försök till sådana brott samt grovt folkrättsbrott. Fingeravtryck som har tagits fram under utredning av nu nämnda brott bör gallras senast sjuttio år efter registreringen.

Den nuvarande lagstiftningen anger inte någon bestämd tidpunkt för gallring av uppgifter om personer som har lämnat fingeravtryck med stöd av lagen om särskild utlänningskontroll. Av integritetsskäl bör det finnas en i lagen angiven tidpunkt för när uppgifterna senast ska gallras. Vid en avvägning mellan verksamhetsintressen och integritetsintressen framstår tio år som en rimlig gallringsfrist.

Riksarkivet har tidigare föreslagit att det införs en möjlighet att föreskriva om undantag från gallring av samtliga uppgifter som behandlas i fingeravtrycks- eller signalementsregister. *Rikspolisstyrelsen* ställer sig bakom Riksarkivets förslag och menar att fingeravtryck i vart fall bör kunna få bevaras för vetenskapliga ändamål. När det gäller det stora flertalet uppgifter som behandlas i polisens brottsbekämpande verksamhet väger intresset av att bevara uppgifter för historiska, vetenskapliga och statistiska ändamål tillräckligt tungt för att motivera att det skapas en möjlighet att meddela föreskrifter om ett sådant undantag som Riksarkivet har förordat, men i fråga om uppgifter i register över DNA-profiler görs den motsatta bedömningen. I promemorian ifrågasätts om behovet av att bevara uppgifter i fingeravtrycks- och signalementsregister för historiska, statistiska eller vetenskapliga ändamål är särskilt stort, eftersom uppgifterna främst utgör identifieringsuppgifter och inte berättar mycket om vår samtid. Enligt promemorian får integritetsintressena

anses väga tyngre. Mot bakgrund bl.a. av de skäl som Rikspolisstyrelsen framför bör det dock finnas en möjlighet för regeringen, eller för annan myndighet efter delegation av regeringen, att meddela föreskrifter om undantag från bestämmelserna om gallring.

Övriga frågor

I avsnitt 12.3 behandlas frågor om direktåtkomst till registren och i avsnitt 12.4 möjligheten att lämna ut uppgifter på medium för automatiserad behandling. I avsnitt 13 behandlas frågor om sekretess.

15.4 Penningtvättsregister

Regeringens förslag: Rikspolisstyrelsen får behandla uppgifter i penningtvättsregister för att förebygga, förhindra eller upptäcka brottslig verksamhet

1. där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller
2. som innefattar finansiering av terrorism.

Uppgifterna i penningtvättsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Regeringen eller den myndighet som regeringen bestämmer har, trots gallringsbestämmelsen, möjlighet att meddela föreskrifter om att uppgifter får bevaras under längre tid för historiska, statistiska eller vetenskapliga ändamål.

Utredningen lämnar inte något förslag i detta avseende.

Remissinstanserna har inte berört frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna har inget att anföra mot promemorians förslag. *Finansinspektionen* välkomnar tydliga regler för möjligheten att behandla personuppgifter i penningtvättsregistret. *Ekobrottsmyndigheten* anser att myndigheten bör ges direktåtkomst till uppgifterna i penningtvättsregister. *Skatteverket* anser att det finns ett behov av lagstöd för informationsutbyte mellan Skatteverkets brottsbekämpande verksamhet och Finanspolisen. Verket utgår från att det kommer att finnas möjligheter till informationsutbyte, även i form av direktåtkomst, till gemensamt tillgängliga uppgifter som behandlas av Finanspolisen utanför penningtvättsregistret.

Skälen för regeringens förslag: I mars 2009 trädde lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism i kraft. Genom lagen, som ersatte den tidigare lagen (1993:768) om åtgärder mot penningtvätt, genomförs det tredje penningtvättsdirektivet (2005/60/EG).

Med penningtvätt avses enligt 1 kap. 5 § 6 lagen om åtgärder mot penningtvätt och finansiering av terrorism sådana åtgärder med brottsligt förvärvad egendom som kan medföra att egendomens samband med brott döljs, att den brottslige får möjlighet att undandra sig rättsliga påföljder eller att återskaffandet av egendomen försvåras, samt sådana åtgärder som innefattar förfogande över och förvärv, innehav och brukande av

egendomen. Med penningtvätt avses även sådana åtgärder med annan egendom än som nyss nämnts, om åtgärderna är ägnade att dölja att någon har berikat sig genom brottslig gärning.

De förfaranden som enligt lagen utgör penningtvätt är straffbelagda i 9 kap. 6–7 a §§ brottsbalken som häleri eller penninghäleri.

Med finansiering av terrorism avses enligt 1 kap. 5 § 4 lagen om åtgärder mot penningtvätt och finansiering av terrorism insamling, tillhandahållande eller mottagande av tillgångar i syfte att de ska användas eller med vetskap om att de är avsedda att användas för att begå sådan brottslighet som avses i 2 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall. Sistnämnda lag innehåller straffrättsliga bestämmelser som genomför konventionen om bekämpande av finansiering av terrorism (SÖ 2002:44).

Verksamhetsutövare som omfattas av lagen om åtgärder mot penningtvätt och finansiering av terrorism är enligt 3 kap. 1 § samma lag skyldiga att granska ekonomiska transaktioner för att kunna upptäcka sådana transaktioner som verksamhetsutövaren misstänker eller har skälig grund att misstänka utgör ett led i penningtvätt eller finansiering av terrorism. Om misstanken kvarstår efter närmare analys, ska uppgifter om alla omständigheter som kan tyda på penningtvätt eller finansiering av terrorism utan dröjsmål lämnas till Rikspolisstyrelsen. Vidare ska, enligt 3 kap. 6 § samma lag, en tillsynsmyndighet som vid en inspektion eller på annat sätt upptäcker en omständighet som kan antas ha samband med eller utgöra penningtvätt eller finansiering av terrorism, underrätta Rikspolisstyrelsen om detta. Inom Rikspolisstyrelsen är en särskild enhet, Finanspolisen, ansvarig för hanteringen av sådana uppgifter som lämnas enligt lagen. Finanspolisen ska alltså ta emot uppgifter som kan tyda på penningtvätt eller finansiering av terrorism.

De uppgifter som Finanspolisen tar emot av anmälningspliktiga organ behandlas i ett särskilt analys- och spaningsregister (se *bilaga 6*). När Finanspolisen tar emot en uppgift är det inte klarlagt om den transaktion som uppgiften avser över huvud taget utgör brott eller brottslig verksamhet. Även om sådana uppgifter i och för sig torde rymmas inom lagens allmänna ändamål i 2 kap. 7 och 9 §§, har de inte alltid det nödvändiga sambandet med konkreta brott eller med brottslig verksamhet som krävs för att få göra uppgifterna gemensamt tillgängliga. Det kan ibland krävas omfattande bearbetning av de anmälda uppgifterna innan transaktionerna kan knytas till brott eller brottslig verksamhet. Mot bakgrund härav bör det införas särskilda bestämmelser för den behandling som Finanspolisen utför i detta avseende.

Inom ramen för arbetet med att bekämpa penningtvätt och finansiering av terrorism tar Finanspolisen även emot uppgifter om misstänkta transaktioner från motsvarande enheter vid utländska myndigheter. Vidare tar Finanspolisen emot underrättelseinformation från övriga polisen och andra myndigheter samt uppgifter i anmälningar och tips från allmänheten. Den nya lagen bör ge stöd även för sådan behandling.

Som föreslås i promemorian bör det således i den nya lagen finnas bestämmelser som ger Rikspolisstyrelsen möjlighet att behandla uppgifter i särskilda register för att förebygga, förhindra och upptäcka dels brottslig verksamhet där penningtvätt utgör ett led för att dölja vinning av brott eller brottslig verksamhet, dels brottslig verksamhet som innefattar finan-

siering av terrorism. Sådana register bör lämpligen benämnas penningtvättsregister.

Vid Finanspolisen tjänstgör för närvarande ca 15 personer och det är endast dessa personer som har åtkomst till uppgifterna i penningtvättsregister. Rikspolisstyrelsen har under hand uppgett att det även i framtiden kommer att vara endast ett mindre antal personer inom polisen som behöver ha tillgång till uppgifterna för att kunna utföra sina arbetsuppgifter. Med hänsyn till detta behövs det inte några bestämmelser om särskilda upplysningar eller om sökbegränsningar för uppgifter som behandlas i penningtvättsregister.

Som föreslås i promemorian bör det införas en särskild bestämmelse om gallring. I lagen om åtgärder mot penningtvätt och finansiering av terrorism föreskrivs att en verksamhetsutövare ska bevara vissa handlingar och uppgifter i minst fem år (2 kap. 13 §). Syftet med bestämmelsen är att verksamhetsutövaren ska bevara uppgifter som har betydelse för kontrollen av misstankar om penningtvätt eller finansiering av terrorism under viss tid. En särskild gallringsregel som tar hänsyn till denna bestämmelse bör tas in i den nya lagen. Uppgifter i penningtvättsregister bör därför gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Regeringen eller den myndighet som regeringen bestämmer bör få meddela föreskrifter om att uppgifter trots gallringsbestämmelsen ska bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande reglering föreslås för behandling av uppgifter för liknande ändamål i andra delar av lagen, nämligen för att förebygga, förhindra och upptäcka brottslig verksamhet. Det finns inte skäl att föreslå någon annan lösning för den behandling som sker med anledning av misstänkt penningtvätt eller finansiering av terrorism.

Ekobrottsmyndigheten anför att myndigheten behöver direktåtkomst till uppgifter i penningtvättsregister. Som framgår av avsnitt 12.3.3 är uppgifterna i penningtvättsregister av sådan art att andra myndigheter inte bör kunna få direktåtkomst till ett sådant register. I avsnitt 12.4 behandlas möjligheten att lämna ut uppgifter ur ett sådant register på medium för automatiserad behandling.

Att direktåtkomst inte tillåts hindrar dock inte att Finanspolisen lämnar information som finns i penningtvättsregister till andra brottsbekämpande myndigheter på annat sätt. Det hindrar inte heller att annan information än sådan som finns i penningtvättsregister lämnas ut till andra brottsbekämpande myndigheter genom direktåtkomst eller på annat sätt. *Skatteverket* pekar på att det finns ett behov av lagstöd för sådant informationsutbyte. I avsnitt 7.6 redogörs för de bestämmelser i den föreslagna lagen som möjliggör sådant informationsutbyte.

15.5 Det internationella registret

Regeringens förslag: Rikspolisstyrelsen får behandla uppgifter i ett internationellt register, om det behövs för att ta emot och besvara ärenden som rör internationellt polissamarbete eller att bistå andra myndigheter i kontakter angående internationellt straffrättsligt samarbete. Detsamma ska gälla om uppgifter måste behandlas för att en svensk begäran om internationellt samarbete eller om rättslig hjälp ska kunna hanteras. Även vissa andra ärenden, som enligt en internationell överenskommelse ska handläggas av polisen, får behandlas i registret. Uppgifter i registret ska gallras senast tre år efter utgången av det kalenderår då ärendet i vilket uppgifterna behandlades avslutades. Regeringen eller den myndighet som regeringen bestämmer har, trots gallringsbestämmelsen, möjlighet att meddela föreskrifter om att uppgifter får bevaras under längre tid för historiska, statistiska eller vetenskapliga ändamål.

Utredningen behandlar inte frågan om ett särskilt register för internationella ärenden.

Remissinstanserna har inte framfört några synpunkter i ämnet.

Promemorian innehåller inte något förslag om ett särskilt register för internationella ärenden.

Remissinstanserna: *Rikspolisstyrelsen* framhåller att det finns påtagliga problem med den föreslagna lagstiftningen när det gäller det dokument- och ärendehanteringssystem (DAR II) som används för ärenden om internationella frågor vid Rikskriminalpolisen. Ett problem är att både personuppgiftslagen och den föreslagna nya lagen ska gälla för DAR II, eftersom det förekommer viss ärendehantering som ligger vid sidan av brottsbekämpningen som exempelvis konsulära ärenden och ärenden som rör dödsfall i utlandet. Andra problem är förslagen om sökbegränsningar och gallring.

Skälen för regeringens förslag

Handläggningen av internationella ärenden

Rikspolisstyrelsen har huvudansvaret för polisens internationella kontakter. Enheten för internationellt polissamarbete vid Rikskriminalpolisen (i fortsättningen kallad internationella enheten) är nationell kontaktpunkt för samarbetet enligt ett flertal internationella överenskommelser. Internationella enheten, som består av cirka 80 personer, fungerar som kontaktpunkt både när det gäller samarbetet med Interpol och det europeiska samarbetet inom Europol. I egenskap av kontaktpunkt tar enheten emot förfrågningar från Interpol och Europol och från andra stater som deltar i polissamarbetet. Förfrågningarna kan exempelvis gälla uppgifter ur belastningsregistret och misstankeregistret. Ibland kan förfrågningarna besvaras direkt, t.ex. genom en registerslagning. I andra fall vidarebefordrar enheten frågan till en lokal polismyndighet, åklagare eller annan som frågan riktar sig till. I vissa fall begärs en konkret åtgärd, t.ex. förhör med eller delgivning av en viss person. Sådana framställningar vidarebefordras på motsvarande sätt. Svaren och resultaten av begärda åtgärder

förmedlas samma väg, dvs. de går via den internationella enheten till den som har ställt frågan eller begärt hjälp med viss åtgärd.

Den internationella enheten fungerar också som mottagare och förmedlare av underrättelseinformation framför allt till och från Europol. Vid internationella enheten finns det svenska Sirenekontoret. Detta ansvarar för kontakterna inom Schengensamarbetet och för hanteringen av den svenska delen av Schengen Information System (SIS). Enheten fungerar som kontaktpunkt när överlämnande enligt den europeiska arresteringsordern aktualiseras, eftersom efterlysning i de fallen kan göras genom SIS. SIS är ett efterlysnings- och spaningshjälpmedel för polissamarbetet inom EU. Norge, Island och Schweiz deltar också i detta samarbete. Registret beskrivs närmare i departementspromemorian SIS II – en andra generation av Schengens informationssystem (Ds 2008:81 s. 53). I departementspromemorian föreslås att betydligt fler uppgifter ska registreras i SIS, bl.a. s.k. tilläggsinformation (Ds 2008:81 s. 100 f.) Som redovisats i avsnitt 6.3 ligger behandling i SIS-registret utanför tillämpningsområdet för den nya lagen. Den behandling av uppgifter inom ramen för Schengensamarbetet som inte avser registrering i SIS omfattas dock.

Enheten är också nationell kontaktpunkt vid informationsutbyte enligt förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter inom EU och för visst annat EU-samarbete. Nyligen har en utredare föreslagit att Rikspolisstyrelsen ska utses till kontaktpunkt för den polissamverkan som ska äga rum med stöd av Prümrådsbeslutet (Ds 2009:8 s. 142). Avsikten är att lägga även denna uppgift på den internationella enheten.

Enheten förmedlar även förfrågningar från den svenska polisen till stater utanför Norden samt till Europol och Interpol. Samarbetet inom Norden sker huvudsakligen genom direktkontakt mellan berörda myndigheter. I viss utsträckning bistår enheten även åklagare och andra brottsbekämpande myndigheter med internationella kontakter i brottmålsfrågor. Man bistår också vissa andra myndigheter, som Migrationsverket, i frågor med anknytning till den polisiära verksamheten.

Ett huvudskäl till att den internationella enheten fungerar som nationell kontaktpunkt i så många olika sammanhang är att enheten är bemannad dygnet runt, vilket inte sällan ställs som krav i internationella överenskommelser om polissamarbete.

Den internationella enheten hanterar ett mycket stort antal ärenden årligen. Ärendena hanteras i ett dokument- och ärendehanteringssystem benämnt DAR II (se *bilaga 6*). Rikspolisstyrelsen uppger att det under år 2007 inkom drygt 43 000 elektroniska meddelanden (här kallade ärenden) till enheten via Interpols kommunikationssystem I 24/7. Fler än 6 000 ärenden skickades till Interpol. Till Sirenekontoret inkom cirka 44 000 ärenden, medan drygt 5 000 ärenden skickades från kontoret.

Utöver vad som har redovisats ovan skapades cirka 30 000 nya ärenden i DAR II under samma år. DAR II används för diarieföring och i princip all hantering av dokument och ärenden vid den internationella enheten.

Enligt Rikspolisstyrelsen händer det att förfrågningar från utlandet om samma sak ställs via olika kanaler, exempelvis Interpol och Schengen. Då är det enligt styrelsen viktigt att kunna koppla samman förfrågningarna och behandla dessa vid ett tillfälle och på ett enhetligt sätt.

Ett särskilt register behövs

Det polisiära samarbetet, särskilt inom EU, utvecklas snabbt. Det ställs i allt större utsträckning krav på korta handläggningstider och effektivt informationsutbyte. Som exempel kan nämnas kraven i flera överenskommelser på att en nationell kontaktpunkt ska finnas tillgänglig dygnet runt, året om. Som framgått ovan fullgör den internationella enheten, som en del av Rikspolisstyrelsen, den uppgiften. För att kontaktpunkten ska kunna fungera effektivt krävs det ett bra verksamhetsstöd. Detta verksamhetsstöd måste, inte minst med tanke på det stora ärendeflödet, anpassas till enhetens speciella uppgifter. Den internationella enheten fungerar i huvudsak som brevlåda och knutpunkt när det gäller såväl förfrågningar från svenska myndigheter som förfrågningar till svenska myndigheter. Däremot sysslar man inte med vare sig underrättelsearbete eller annan direkt brottsbekämpande verksamhet.

Det bör också framhållas att verksamheten vid internationella enheten ofta avser allmänna förfrågningar eller allmän information om det svenska rättssystemet som inte direkt kan hänföras till ett visst brott eller viss brottslig verksamhet. Verksamheten innefattar också i stor utsträckning mottagande av information som sänds till samtliga stater som deltar i Interpol- eller Europolsamarbetet och som inte sällan helt saknar betydelse för den svenska polisen. Samtidigt förekommer personuppgifter frekvent i informationsflödet.

Uppgifterna i internationella ärenden behöver vara tillgängliga för ett flertal personer, med tanke på de ökande kraven på att förfrågningar ska besvaras snabbt (i vissa fall inom 24 timmar eller ännu snabbare). Så korta svarstider innebär att var och en inom enheten måste kunna ta över handläggningen av ett ärende från någon annan. Uppgifterna måste således vara gemensamt tillgängliga.

Mot denna bakgrund fungerar, som *Rikspolisstyrelsen* påpekar, vissa av bestämmelserna i promemorians förslag mindre väl för den verksamhet som förekommer vid den internationella enheten. Detta gäller bl.a. bestämmelserna om sökbegränsningar och gallring. Det krävs därför en särlösning för att tillgodose de krav som handläggningen av internationella ärenden ställer.

I den nya lagen bör det tas in bestämmelser som ger Rikspolisstyrelsen möjlighet att behandla uppgifter i ett särskilt register över internationella ärenden, det internationella registret. Huvudändamålet med detta bör vara att stödja Rikspolisstyrelsens uppgift som avsändare och mottagare av information i det polisiära samarbetet avseende brottsbekämpning. Reglerna måste utformas så att Sveriges internationella förpliktelser kan uppfyllas. Det förhållandet att enheten tar emot olika typer av internationella uppgifter innebär att det kan röra sig såväl om uppgifter om brott som underrättelseinformation. Det måste därför vara möjligt att behandla alla inkommande uppgifter i registret, oavsett vilken karaktär dessa har. All fortsatt behandling, t.ex. analys av mottagen underrättelseinformation eller utredning av ett påstått brott, ska göras utanför registret. Däremot får uppgifter om resultatet, t.ex. ett förhörsprotokoll eller resultatet av en viss analys, behandlas i registret som ett led i återredovisningen till den stat som har begärt åtgärden eller initierat förfrågan.

Som nyss nämnts bistår Rikspolisstyrelsen också andra myndigheter inom rättsväsendet i frågor som rör straffrättsligt samarbete framför allt utanför EU-området, t.ex. förmedlar kontakter med utländska polismyndigheter. Man hjälper också åklagare och domstolar i enskilda ärenden med exempelvis att få sakuppgifter kontrollerade, adressuppgifter till personer som ska höras eller handlingar delgivna.

Rikspolisstyrelsen fungerar också i vissa särskilda fall som en länk i förhållande till Utrikesdepartementet och andra svenska myndigheter, även om det primärt inte finns någon misstanke om brott. Detta gäller bl.a. vid dödsfall utomlands och om en utländsk myndighet begär brådskande hjälp med att t.ex. identifiera personer som fallit offer för olyckor. De nu aktuella ärendena utgör en mycket liten andel av verksamheten. Vidare hanterar den internationella enheten information om personer som har försvunnit utomlands (och som kan ha fallit offer för brott) och uppgifter om oidentifierade kroppar som har påträffats utomlands. Ändamålen med registret bör även omfatta behandlingen av sådana internationella ärenden. Detta ligger i linje med att det tidigare förslagits att uppgifter om att personer har anmälts som försvunna ska kunna behandlas med stöd av lagen och att DNA- och fingeravtrycksregister får användas för identifiering även i vissa andra fall än vid brottsbekämpning.

I avsnitt 9.6 berörs i korthet behovet av att kunna behandla DNA-profiler i det internationella registret. När det informationsutbyte som krävs enligt Prümrådsbeslutet är fullt utbyggt ska referensuppgifter avseende DNA-profiler kunna utbytas automatiskt mellan medlemsstaterna inom EU. Informationsutbytet ska gå via en nationell kontaktpunkt, som föreslås bli den internationella enheten vid Rikspolisstyrelsen. Det bör dock framhållas att det informationsutbytet främst avser förmedling av referensuppgifter som inte avslöjar identiteten hos den som DNA-profilen tillhör. Det förekommer även utbyte av DNA-profiler med andra stater än de som deltar i Prümsamarbetet. Mot den bakgrunden finns det behov av att kunna behandla DNA-profiler i det internationella registret.

De uppgifter som bör få behandlas i registret är således dels uppgifter som krävs för att Rikspolisstyrelsen ska kunna fungera som mellanhand i det polisiära och rättsliga samarbetet, dels uppgifter i vissa frågor av konsulär art.

Eftersom ett begränsat antal personer kommer att ha tillgång till registret och detta främst ska fungera som ett verksamhetsstöd för mottagning och vidareförmedling av uppgifter där skälet till att uppgifterna behandlas som regel framgår av sammanhanget, finns det inte något behov av att införa bestämmelser om särskilda upplysningar eller sökbegränsningar för uppgifter i registret.

I avsnitt 12.3.3 behandlas frågan om direktåtkomst till registret och i avsnitt 12.4 möjligheten att lämna ut uppgifter ur registret på medium för automatiserad behandling. Någon möjlighet till direktåtkomst föreslås inte.

När det gäller gallring behövs en särskild reglering för det internationella registret. *Rikspolisstyrelsen* framhåller att ett års gallringstid – som föreslås gälla generellt för internationella ärenden – är alltför kort, bl.a. med hänsyn till att handläggaren kan avsluta ärendet när en fråga från utlandet har besvarats. Om utredningen fortsätter i det andra landet och kompletterande information begärs när det förflutit något år kommer,

med en gallringstid om ett år, ärendet inte längre att kunna återfinnas. Rikspolisstyrelsen anser att gallring bör ske först efter tre år.

Eftersom internationella ärenden ibland löper över lång tid, t.ex. när det finns en internationell efterlysning på en person som är misstänkt för allvarliga brott där preskriptionstiden är lång, måste det vara möjligt att behandla och återfinna uppgifter under längre tid än vad som generellt medges i fråga om ärendehantering. Likaså kan ett ärende dra ut på tiden beroende på handläggningstiden i ett annat land. En särskild gallringsbestämmelse som tar hänsyn till detta bör införas. Vid en avvägning mellan verksamhetsintressen och integritetsintressen framstår en regel om gallring tre år efter utgången av det kalenderår då ärendet avslutades som rimlig.

Av de skäl som anges i avsnitt 15.3 och 15.4 bör regeringen, eller den myndighet som regeringen bestämmer, kunna meddela föreskrifter om undantag från bestämmelsen om gallring för bevarande för historiska, statistiska eller vetenskapliga ändamål.

16 Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

16.1 Bakgrund

16.1.1 Säkerhetspolisens verksamhet

Säkerhetspolisen ingår i Rikspolisstyrelsen men har en egen organisation. Av 4 § förordningen (1989:773) med instruktion för Rikspolisstyrelsen framgår att Säkerhetspolisen bedriver polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet m.m. I förordningen (2002:1050) med instruktion för Säkerhetspolisen preciseras dess uppgifter och organisation. Utöver att förebygga och avslöja brott mot rikets säkerhet ska Säkerhetspolisen bl.a. bekämpa terrorism, skydda personer i den centrala statsledningen och fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Säkerhetspolisens verksamhet syftar till att skydda det demokratiska systemet, medborgarnas fri- och rättigheter och den nationella säkerheten.

Verksamheten delas in i fem huvudområden. Kontraspionageverksamheten har till uppgift att förebygga och avslöja spioneri, olaglig underrättelseverksamhet och andra brott mot rikets säkerhet. För att förebygga och avslöja olaglig underrättelseverksamhet mot Sverige och svenska intressen bedriver myndigheten operativt fältarbete samt arbetar med analyser och kontakter med olika delar av det svenska samhället. I arbetet ingår också att avslöja flyktingspionage och annan förföljelse av utlänningar i Sverige från utländska regimer och organisationer.

Inom kontraterrorismverksamheten har Säkerhetspolisen till uppgift att förebygga och avslöja terrorism som riktas mot Sverige eller utländska intressen här i landet, terroristhandlingar i andra länder samt förekomsten av internationella terroristnätverks förgreningar i Sverige. I denna verk-

samhet ingår också att förebygga och utreda brott vid handel med produkter som kan användas för att framställa massförstörelsevapen.

Säkerhetspolisens författningsskyddande verksamhet syftar till att förebygga och avslöja brott mot rikets inre säkerhet, dvs. olaglig verksamhet som syftar till att med våld, hot eller tvång ändra vårt statsskick, förmå beslutande politiska organ eller myndigheter att fatta beslut i en viss riktning eller att hindra enskilda medborgare från att utöva sina grundlagsfästa fri- och rättigheter. Inom ramen för den författningsskyddande verksamheten kartläggs också brott som används som medel för att uttrycka en politisk åsikt eller för att uppnå ett politiskt mål.

Hos Säkerhetspolisen bedrivs även personskyddsverksamhet i form av bevaknings- och säkerhetsarbete. Verksamheten omfattar skyddet av den centrala statsledningen. Till den centrala statsledningen räknas statschefen, riksdagen, regeringen samt statssekreterarna och kabinettssekreteraren. I kretsen av personer som ska skyddas ingår även personer som vistas här i samband med statsbesök och de som omfattas av s.k. annat personskydd. Med det sistnämnda avses skydd som Säkerhetspolisen handhar efter särskilt beslut, som skydd av kungafamiljen och främmande stats beskickningsmedlemmar.

Inom säkerhetsskyddsverksamheten arbetar man för att höja säkerhetsnivån i samhället. Säkerhetspolisen ger råd till och kontrollerar myndigheters och företags verksamhet. Syftet är att skydda mot spionieri, sabotage och andra brott som kan röra rikets säkerhet, att skydda hanteringen av uppgifter som har betydelse för rikets säkerhet och att förebygga terrorism. I arbetet ingår att genomföra registerkontroll av personer efter framställan från berörda myndigheter eller i vissa fall annan stat eller mellanfolklig organisation.

Tyngdpunkten i Säkerhetspolisens verksamhet ligger på förebyggande arbete.

16.1.2 Säkerhetspolisens nuvarande behandling av personuppgifter

Säkerhetspolisens behandling av personuppgifter sker med stöd av bestämmelserna i personuppgiftslagen (1998:204) och den allmänna delen av polisdatalagen (1998:622), dvs. 1–9 och 13 §§. Utöver detta finns det särskilda bestämmelser om det s.k. SÄPO-registret i 32–35 §§ polisdatalagen och 12 och 13 §§ polisdataförordningen (1999:81). Bestämmelserna innebär att det ska föras ett SÄPO-register som har till ändamål att underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet och bekämpa terroristbrott samt utgöra underlag för registerkontroll enligt säkerhetsskyddslagen. I polisdatalagen anges vilka uppgifter som får föras in i registret och när dessa ska gallras. Bestämmelserna i 10 och 11 §§ om behandling av uppgifter om kvarstående misstankar och 14–21 §§ polisdatalagen om kriminalunderrättelseverksamhet gäller inte för Säkerhetspolisen.

Säkerhetspolisen för bl.a. ett centralregister samt särskilda uppgiftssamlingar för bearbetning och analys av underrättelseinformation. Dessutom förs diarier.

Centralregistret utgör ett arbetsverktyg i vilket behöriga befattningshavare för in uppgifter genom att bearbeta avslutade ärenden och göra uppgifterna sökbara. Endast sådana uppgifter som enligt 33 och 34 §§ polisdatalagen får finnas i SÄPO-registret registreras. Tillgången till uppgifter i centralregistret begränsas till vad var och en behöver för att kunna utföra sina arbetsuppgifter (jfr 13 § polisdataförordningen). För att få behörighet till registret måste personalen genomgå en utbildning som avslutas med ett prov, som måste vara godkänt. Behörigheten delas upp i olika nivåer beroende på vilka behov den anställde har.

De enskilda handlingarna i varje ärende finns inte i centralregistret men kan nås via registret genom en sökning på ärendet. En förutsättning för att en tjänsteman ska få tillgång till handlingarna i ett ärende är att denne är behörig. I varje ärende finns det uppgift om uppgiftslämnarens tillförlitlighet. Där anges vidare om uppgifterna bygger på uppgiftslämnarens egna iakttagelser eller om det är fråga om andrahandsuppgifter. Dessutom klassificeras uppgifternas tillförlitlighet enligt ett särskilt system. Alla transaktioner och frågor i centralregistret loggas. Enhetscheferna kontrollerar regelbundet den egna personalens loggningar i registret. En särskild enhet utför daglig kontroll av all uppdatering som görs i centralregistret. Beslut om nyregistrering av en fysisk eller juridisk person i centralregistret fattas av den enhetschef som ansvarar för dokumentation. Gallring genomförs av enheten för dokumentation efter yttrande från ansvarig enhet. Den ansvariga enheten bevakar gallringsfrister och begär vid behov förlängd gallringstid enligt 35 § första stycket polisdatalagen.

För bearbetning och analys av underrättelser behandlas personuppgifter även i avgränsade uppgiftssamlingar. En närmare beskrivning av de databaser och ärendehanteringssystem som förs hos Säkerhetspolisen finns i *bilaga 6.*

Inom Säkerhetspolisen pågår arbete med att ta fram ett nytt ärendehanteringssystem.

16.1.3 Extern kontroll av personuppgiftsbehandlingen

Datainspektionen utövar tillsyn över Säkerhetspolisens behandling av personuppgifter inom den brottsbekämpande verksamheten enligt samma regler som gäller för alla myndigheter. Därutöver har Säkerhets- och integritetsskyddsnämnden, som den 1 januari 2008 övertog Registernämndens uppgifter, till uppgift att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen, särskilt med avseende på 5 § som reglerar behandling av känsliga personuppgifter (1 § andra stycket lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). I avsnitt 17.2 redogörs närmare för tillsynen över polisens personuppgiftsbehandling.

Nämnden utövar tillsyn såväl på eget initiativ som på begäran av en enskild. Vid nämndens tillsyn på eget initiativ används både slumpmässiga urval och riktade urval av områden där det bedöms finnas en påtaglig risk för felaktigheter. Nämnden är skyldig att på begäran av en enskild kontrollera bl.a. om han eller hon i strid med lag eller annan författning har varit föremål för Säkerhetspolisens personuppgiftsbehandling.

När kontrollen har utförts ska nämnden underrätta den enskilde om detta. Skulle nämnden vid en kontroll finna att Säkerhetspolisen har behandlat personuppgifter i strid med gällande författningar ska den person som har begärt kontrollen underrättas även om detta. Nämnden är då också skyldig att anmäla den författningsstridiga verksamheten till Justitiekanslern, Åklagarmyndigheten, Datainspektionen eller någon annan behörig myndighet för åtgärd.

Inrättandet av Säkerhets- och integritetsskyddsnämnden har medfört att möjligheten för enskilda att begära en kontroll av Säkerhetspolisens personuppgiftsbehandling har ökat.

16.2 Utgångspunkterna för regleringen

16.2.1 Huvuddragen i den nya regleringen

Regeringens förslag: På grund av särdragen i Säkerhetspolisens verksamhet införs särskilda bestämmelser för behandlingen av personuppgifter i dess brottsbekämpande verksamhet.

Regeringens bedömning: Bestämmelserna om Säkerhetspolisens behandling av personuppgifter bör i huvudsak ha samma innebörd som gällande rätt.

Utredningen föreslår ett mindre antal särbestämmelser för Säkerhetspolisen. Utredningens bedömning överensstämmer i huvudsak med promemorians.

Remissinstanserna har inte haft något att invända mot utredningens förslag. Dåvarande *Registernämnden* har vitsordat att SÄPO-registret inte längre behöver föras i den form som polisdatalagen kräver.

Promemorians förslag och bedömning överensstämmer med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget i stort. Vissa detaljsynpunkter framförs dock. Remissinstanserna tillstyrker eller har inget att invända mot promemorians bedömning.

Skälen för regeringens förslag och bedömning: Säkerhetspolisens verksamhet bedrivs i stor utsträckning på liknande sätt som verksamheten vid polisen i övrigt. Den reglering som föreslås för polisen i övrigt bör därför i många avseenden tillämpas även på Säkerhetspolisens verksamhet. Särdragen i Säkerhetspolisens verksamhet motiverar dock att vissa bestämmelser, liksom hittills, utformas på ett sätt som är särskilt anpassat till denna verksamhet. I motsats till vad som gäller för polisen i övrigt är Säkerhetspolisens brottsutredande verksamhet mycket liten. Tyngdpunkten ligger i stället på underrättelseverksamhet och renodlat förebyggande arbete.

Säkerhetspolisen behöver behandla personuppgifter på ett i huvudsak oförändrat sätt. Bestämmelserna om Säkerhetspolisens behandling av personuppgifter bör därför i huvudsak ha samma innebörd som gällande rätt. Utöver de föreskrifter som finns i lag och förordning har Säkerhetspolisen utarbetat interna bestämmelser för att garantera ett starkt skydd för enskilda som registreras. Skyddet kontrolleras och utvärderas löpande

såväl inom myndigheten som av Säkerhets- och integritetsskyddsnämnden.

Regeringen delar Polisdatautredningens och promemorians uppfattning att den nya lagen inte bör innehålla några bestämmelser om SÄPO-registret. Lagen bör så långt möjligt vara teknikneutral och reglera behandlingen av personuppgifter, inte arbetsmetoderna. Som beskrivs i avsnitt 6.1 går utvecklingen mot att behandling av personuppgifter i traditionella register överges och att sådan behandling i stället sker i mer avancerade datasystem. På samma sätt som för polisen i övrigt bör det i den nya lagen införas särskilda bestämmelser om uppgifter som görs eller har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet. Dessa bestämmelser syftar till att skydda den personliga integriteten för berörda personer, bl.a. genom att säkerställa att det tydligt framgår varför en personuppgift behandlas.

Som anförs i promemorian bör bestämmelserna i den nya lagen endast ge ramen för den tillåtna personuppgiftsbehandlingen. Ingen remissinstans har ifrågasatt denna utgångspunkt. En sådan reglering innebär emellertid att det i stor utsträckning överlåts till Säkerhetspolisen att avgöra hur insamlade uppgifter ska struktureras, göras åtkomliga och behandlas i verksamheten. För att detta ska vara acceptabelt från integritetsskyddssynpunkt krävs att verksamheten fortlöpande kontrolleras av någon med särskild insyn i verksamheten. *Justitiekanslern* pekar i sitt remissvar på att det såväl historiskt som i modern tid har funnits problem med insyn i Säkerhetspolisens registerhantering och hänvisar till betänkandena Rikets säkerhet och den personliga integriteten (SOU 2002:87) och Politisk övervakning och personkontroll 1969–2002 (SOU 2002:89). Justitiekanslern framhåller vidare att Europadomstolen i en dom den 6 juni 2006 har funnit att Sverige brutit mot ett antal grundläggande fri- och rättigheter i Europakonventionen genom viss lagring av personuppgifter hos Säkerhetspolisen (Segerstedt-Wiberg m.fl. mot Sverige). Enligt regeringens bedömning utgör inrättandet av Säkerhets- och integritetsskyddsnämnden, vilket skett bl.a. mot bakgrund av Europadomstolens dom, och den tillsyn som nämnden bedriver en bra grund för att värna integritetsskyddet. Utöver denna särskilda tillsyn utövar Datainspektionen sedvanlig tillsyn över personuppgiftsbehandlingen (se avsnitt 17.2). Sammantaget tillgodoses därmed integritetsskyddsintressena på ett tillfredsställande sätt.

I det följande redovisas hur bestämmelserna för behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet bör utformas.

16.2.2 Bestämmelser som ska gälla även för Säkerhetspolisen

Regeringens förslag: Huvuddelen av de bestämmelser som föreslås gälla i polisens brottsbekämpande verksamhet i övrigt ska gälla även i Säkerhetspolisens verksamhet, däribland bestämmelserna om

– förhållandet till personuppgiftslagen (1998:204),
– tillsyn,
– behandlingen av känsliga personuppgifter,
– tillgången till uppgifter, och
– utlämnande av uppgifter till bl.a. utländsk myndighet.

Vidare ska bestämmelser med i huvudsak samma innebörd som motsvarande bestämmelser för polisen i övrigt gälla i fråga om behandlingen av uppgifter om juridiska personer och personuppgiftsansvar. Personuppgifter som behandlas automatiserat i Säkerhetspolisens verksamhet får inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som gäller för Säkerhetspolisens behandling av personuppgifter. Vidare ska samma regler gälla för Säkerhetspolisen som för polisen i övrigt när det gäller gallring av uppgifter som inte har gjorts gemensamt tillgängliga samt vissa andra bestämmelser om bevarande och gallring.

Utredningens förslag: Utredningen väljer en annan lagteknisk lösning. I sak överensstämmer dock utredningens förslag i allt väsentligt med promemorians.

Remissinstanserna: Dåvarande *Registernämnden* har ifrågasatt om det kommer att vara möjligt att undvika att känsliga personuppgifter kommer att behandlas på ett otillåtet sätt, bl.a. i de s.k. analysdatabaserna. Övriga remissinstanser har inte yttrat sig särskilt i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens**.** Promemorian föreslår dock inte någon uttrycklig bestämmelse som anger att uppgifter aldrig får bevaras längre än vad som behövs för något eller några av de ändamål som gäller för Säkerhetspolisens personuppgiftsbehandling.

Remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Säkerhetspolisen* efterlyser dock ett klargörande av när myndigheten omfattas av lagens bestämmelser.

Skälen för regeringens förslag: Åtskilliga av de bestämmelser som föreslås gälla för den övriga polisens behandling av personuppgifter bör gälla även för Säkerhetspolisen. Till dessa hör bestämmelserna om lagens tillämpningsområde (avsnitt 6.3). Detsamma gäller förhållandet till personuppgiftslagen och tillämpliga bestämmelser i personuppgiftslagen (avsnitt 6.4). Vidare bör, som föreslås i avsnitt 17.2, gälla i huvudsak samma bestämmelser om tillsyn över behandlingen av personuppgifter som för polisen i övrigt.

I avsnitt 8 föreslås bestämmelser som begränsar möjligheten att behandla känsliga personuppgifter. Också dessa bör gälla vid personuppgiftsbehandling i Säkerhetspolisens verksamhet. Registernämnden ifrågasatte i sitt remissyttrande över Polisdatautredningens betänkande om de regler som utredningen föreslagit var tillräckliga för att förhindra otillåten behandling av känsliga personuppgifter. Senare utarbetade Säkerhetspolisen en särskild rutin för registreringen av känsliga person-

uppgifter vilken accepterades av Registernämnden. Syftet var att undvika att känsliga personuppgifter behandlas i strid med gällande regler. Av Registernämndens verksamhetsberättelse för år 2007 framgår att nämnden särskilt granskade samtliga nyregistreringar i centralregistret på kontraterrorismens område under en månads tid. Vid inspektionen påträffades inte några registreringar som stred mot 5 § polisdatalagen. Säkerhetspolisens behandling av känsliga personuppgifter har under år 2008 varit föremål för Säkerhets- och integritetsskyddsnämndens granskning i ett stort antal fall. Av nämndens årsberättelse för år 2008 framgår att granskningen inte har påvisat några brister i behandlingen av känsliga personuppgifter med undantag för ett påpekande, vilket föranlett åtgärder från Säkerhetspolisens sida.

Den principiellt viktiga bestämmelsen om att endast de personer i verksamheten som behöver ha tillgång till uppgifter för att kunna fullgöra sina arbetsuppgifter ska ha det (avsnitt 6.6) bör gälla även för Säkerhetspolisen. När det gäller utlämnande av uppgifter till bl.a. utländska myndigheter föreslås i avsnitt 12 att den nya lagen ges ett innehåll som motsvarar nuvarande reglering. Förslaget omfattar även Säkerhetspolisens personuppgiftsbehandling. Vidare bör samma regler gälla för Säkerhetspolisens utlämnande av uppgifter på medium för automatiserad behandling som för polisen i övrigt.

Säkerhetspolisen bör vara personuppgiftsansvarig för den behandling av personuppgifter som sker i dess egen verksamhet. Vidare bör, på samma sätt som för polisen i övrigt, bestämmelserna om Säkerhetspolisens personuppgiftsbehandling i tillämpliga delar gälla för uppgifter om juridiska personer (avsnitt 6.3).

I avsnitt 14.1 redogörs närmare för de allmänna utgångspunkter för bevarande och gallring som föreslås gälla för polisen i övrigt. Där bemöts även den remisskritik som riktas mot promemorians förslag i denna del. De utgångspunkter som anges där bör gälla i tillämpliga delar även för Säkerhetspolisen. Lagen bör således innehålla en bestämmelse som anger att uppgifter inte får bevaras längre än vad som behövs för något eller några av de ändamål som gäller för Säkerhetspolisens behandling av uppgifter. Denna generella bestämmelse bör kompletteras med bestämmelser som föreskriver en yttersta gräns för bevarande av vissa kategorier av personuppgifter. Vidare bör en motsvarande bestämmelse som för polisen i övrigt om gallring av uppgifter som inte har gjorts gemensamt tillgängliga gälla för Säkerhetspolisens personuppgiftsbehandling (avsnitt 14.2). Gallringsbestämmelsen ska på samma sätt som för övriga polisen inte gälla uppgifter i ärenden om utredning eller beivrande av brott. Även vad som anförs i avsnitt 14.1 beträffande digital arkivering bör gälla för Säkerhetspolisen.

När det gäller *Säkerhetspolisens* önskemål om att myndigheten bl.a. ska anges direkt i bestämmelserna och inte ha ställning som polismyndighet alternativt Rikspolisstyrelsen finns det inte skäl att göra någon annan bedömning än den som gjorts i promemorian. I avsnitt 6.3 redovisas skälen för detta.

16.3 Ändamålen med behandlingen

16.3.1 Utgångspunkter

Regeringens förslag: I lagen ska det anges för vilka ändamål Säkerhetspolisen får behandla personuppgifter i den brottsbekämpande verksamheten. Ändamålen ska delas in i primära och sekundära. De primära ändamålen avser behandling av personuppgifter för att tillgodose Säkerhetspolisens egna behov. De sekundära ändamålen avser behandling för att lämna ut personuppgifter. I fråga om behandling av personuppgifter för andra ändamål än de primära eller sekundära gäller den s.k. finalitetsprincipen i 9 § första stycket d personuppgiftslagen.

Utredningens förslag: Personuppgifter ska få behandlas bara om behandlingen är nödvändig för att sådan verksamhet som omfattas av lagen ska kunna utföras. Personuppgifter ska få samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål och senare behandling får inte ske för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft något att invända mot det.

Promemorians förslag överensstämmer delvis med regeringens. Promemorian föreslår emellertid en uttömmande reglering av för vilka ändamål personuppgifter får behandlas och finalitetsprincipen föreslås inte vara tillämplig.

Remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag när det gäller Säkerhetspolisen. Generellt kritiseras dock lagens ändamålsreglering av flera remissinstanser.

Skälen för regeringens förslag: I avsnitt 7.1 redogörs närmare för hur den nya lagens ändamålsreglering bör utformas. Där bemöts den remisskritik som riktas mot promemorians förslag i denna del. Den ändamålsreglering som föreslås i avsnitt 7.1 bör gälla även för Säkerhetspolisen. I lagen bör således göras en uppdelning mellan primära och sekundära ändamål. De primära ändamålen bör anges uttömmande medan de sekundära ändamålen bör anges så tydligt och fullständigt som möjligt och kompletteras med en möjlighet att behandla uppgifter även för ändamål som inte är oförenliga med insamlingsändamålet enligt finalitetsprincipen. I avsnitt 16.3.2 och 16.3.3 redovisas närmare de primära respektive sekundära ändamålen för vilka Säkerhetspolisen bör få behandla personuppgifter.

16.3.2 Primära ändamål

Regeringens förslag: Personuppgifter ska få behandlas i Säkerhetspolisens verksamhet om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terroristbrott samt vissa yttrandefrihetsbrott och tryckfrihetsbrott,
2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra uppgifter i samband med personskydd,
4. fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627),
5. fullgöra de förpliktelser som följer av internationella åtaganden, eller
6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

Personuppgifter ska alltid få behandlas om behandlingen är nödvändig för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Utredningens förslag: Säkerhetspolisen ska få behandla personuppgifter för att underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet, spaning i syfte att bekämpa terrorism samt registerkontroll enligt säkerhetsskyddslagen. Vidare föreslår utredningen en bestämmelse enligt vilken det alltid ska vara tillåtet att diarieföra personuppgifter och behandla dem i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

Remissinstanserna har inte haft någon invändning mot utredningens förslag.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inget att invända mot promemorians förslag. *Justitiekanslern* samt *Säkerhets- och integritetsskyddsnämnden* betonar vikten av att den föreslagna ändamålsregleringen inte kommer i konflikt med bestämmelserna om förbud mot censur i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Skälen för regeringens förslag

Förebygga, förhindra eller upptäcka brott mot rikets säkerhet och terroristbrott

En av Säkerhetspolisens viktigaste uppgifter är att förebygga, förhindra och upptäcka brott mot rikets säkerhet. Vidare ansvarar Säkerhetspolisen för att förebygga, förhindra och upptäcka dels terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, dels brott mot lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall (terrorismfinansieringslagen) samt eventuella andra former av terroristbrott. Säkerhetspolisen måste kunna behandla personuppgifter för att fullgöra denna verksamhet.

Rikspolisstyrelsen har meddelat föreskrifter bl.a. om i vilka fall en utredning alltid ska handhas av eller drivas under medverkan av Säkerhets-

polisen (Rikspolisstyrelsens föreskrifter och allmänna råd om skyldighet för polismyndigheterna att underrätta Säkerhetspolisen om vissa brottsmisstankar m.m.; RPSFS 1999:10, FAP 403–3). Eftersom Säkerhetspolisen enligt dessa föreskrifter i vissa fall handhar eller medverkar i utredningar avseende bl.a. yttrandefrihets- eller tryckfrihetsbrott med rasistiska eller främlingsfientliga motiv har myndigheten även behov av att kunna behandla personuppgifter när det behövs för att förebygga, förhindra eller upptäcka sådana brott. Som *Justitiekanslern* och *Säkerhets- och integritetsskyddsnämnden* betonar får detta givetvis inte inkräkta på bestämmelserna om censurförbud i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Säkerhetspolisen behöver kunna samla in, sammanställa och analysera uppgifter inom kontraspionageverksamheten, kontraterrorismverksamheten och författningsskyddsverksamheten även om uppgifterna inte kan hänföras vare sig till något visst konkret brott eller till någon mer konkret definierad brottslig verksamhet. Som exempel kan nämnas behovet av att inom kontraspionaget fortlöpande kunna följa utvecklingen när det gäller andra nationers närvaro i form av underrättelseagenter här i landet, att kunna övervaka sådana personer och att därvid även behandla personuppgifter. Säkerhetspolisen behöver också, med utgångspunkt i svenska intressen, följa den politiska utvecklingen i andra länder och verksamheten inom vissa grupper, som kan utgöra ett hot mot det svenska samhället eller som kan komma att göra sig skyldiga till terroristbrott. Inom författningsskyddet kan Säkerhetspolisen exempelvis behöva kartlägga hot som riktar sig mot vissa grupper i samhället och fortlöpande följa den hotbild som finns mot vissa myndigheter eller organ. Inom ramen för detta arbete måste Säkerhetspolisen kunna dokumentera och analysera både information av underrättelsekaraktär och annan information av olika slag, såväl från offentliga källor som från polisens eget arbete. Säkerhetspolisens behov av att kunna genomföra och dokumentera olika typer av undersökningar och analyser av företeelser, personer, platser etc. är således stort och skiljer sig i flera avseenden från de behov som finns inom den övriga polisen. Skillnaden är att det inom Säkerhetspolisens brottsförebyggande arbete normalt inte går att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet som inom den övriga polisen. Man kan uttrycka det så att den underrättelseverksamhet som bedrivs inom Säkerhetspolisen till sin natur ofta är sådan att den ligger på ett tidigare stadium än den som bedrivs av polisen i övrigt. Å andra sidan är den, genom Säkerhetspolisens instruktion, inriktad mot ett fåtal, väl avgränsade företeelser av särskilt samhällsfarlig karaktär.

Sammantaget finner regeringen, i likhet med promemorian, att det nu sagda inte hindrar att ändamålsbestämmelsen i denna del utformas på samma sätt som motsvarande bestämmelse för den övriga polisen. Den bör dock begränsas så att den enbart omfattar de typer av brott som Säkerhetspolisen enligt författning ansvarar för.

Utreda och beivra brott mot rikets säkerhet och terroristbrott m.m.

Säkerhetspolisen handlägger ett mindre antal förundersökningar per år (för närvarande drygt ett hundratal). Endast ett fåtal av dessa leder till

lagföring. Detta hör bl.a. samman med att verksamheten till allra största delen består av underrättelsearbete. Underrättelsearbetet leder ibland inte fram till misstanke om ett så konkret brott att förundersökning inleds. I andra fall avslutas en inledd förundersökning t.ex. därför att den person som misstankarna riktar sig mot har lämnat Sverige.

När det har begåtts brott av det slag som Säkerhetspolisen bär ett primärt ansvar för att bekämpa, biträder Säkerhetspolisen åklagaren med genomförandet av förundersökningen. Inom ramen för den verksamheten har Säkerhetspolisen i princip samma behov av att kunna behandla personuppgifter som den övriga polisen. Ändamålsbestämmelsen bör utformas så att den knyter an till de typer av brott som Säkerhetspolisen ansvarar för.

Säkerhetspolisen kan i ett enskilt fall fatta beslut om att förundersökningen beträffande någon annan typ av brott än de nyss nämnda antingen ska handhas av Säkerhetspolisen eller under medverkan av Säkerhetspolisen. Vid vissa typer av brott ska Säkerhetspolisen dessutom alltid underrättas (se RPSFS 1999:10, FAP 403–3). Syftet är att Säkerhetspolisen ska kunna överväga att ta över utredningen eller att medverka i utredningen med sin expertis. Säkerhetspolisen måste naturligtvis kunna behandla personuppgifter i sådana förundersökningar i samma utsträckning som polisen i övrigt. I likhet med vad som föreslås i promemorian bör detta framgå direkt av lagen.

Personskydd

Säkerhetspolisens personskyddsverksamhet berör framför allt den centrala statsledningen och statschefen och dennes familj. Syftet är bl.a. att värna rikets inre säkerhet. Arbetet är förebyggande och syftar ytterst till att förhindra att den som skyddas utsätts för brott riktade mot dennes person. Den får därför anses utgöra en del av Säkerhetspolisens brottsbekämpande verksamhet. Inom ramen för detta förebyggande arbete har Säkerhetspolisen behov av att kunna behandla personuppgifter inte bara rörande den person som skyddas utan också om andra personer, exempelvis sådana som kan utgöra ett potentiellt hot, även om det inte finns någon konkret misstanke om brott eller brottslig verksamhet.

Mot denna bakgrund bör det i den nya lagen anges att Säkerhetspolisen får behandla personuppgifter för att fullgöra uppgifter avseende den del av personskyddet som Säkerhetspolisen ansvarar för enligt sin instruktion eller som Rikspolisstyrelsen har överlämnat till Säkerhetspolisen. Anledningen till att detta ändamål bör nämnas särskilt i lagen, när det gäller Säkerhetspolisen, är att man inte kan förutsätta att de brott som kan komma att riktas mot en person som har personskydd ryms under det fåtal brottstyper som det ingår i Säkerhetspolisens uppdrag att bekämpa.

Säkerhetsskyddslagen

Säkerhetspolisen ska enligt 3 § 1 i sin instruktion fullgöra de särskilda uppgifter som Rikspolisstyrelsen ska utföra enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633), bl.a. registerkontroll och särskild personutredning. Detta säkerhetsskyddsarbete får

anses utgöra en del av Säkerhetspolisens brottsbekämpande verksamhet, eftersom det yttersta syftet med kontrollen är att förebygga att personer som kan innebära ett säkerhetshot får uppdrag som är känsliga från säkerhetssynpunkt. För att fullgöra uppgifterna enligt nämnda författningar måste Säkerhetspolisen kunna bearbeta uppgifter som finns i dess egna datasystem samt samla in och bearbeta uppgifter som härrör från särskilda register hos den övriga polisen och andra uppgifter som den behandlar. Detta ändamål bör anges särskilt i lagen.

Internationellt arbete

För Säkerhetspolisens verksamhet gäller, i stor utsträckning, att verksamheten är beroende av internationellt samarbete. Ett viktigt skäl till detta är att terrorismen i stor utsträckning är internationell. Säkerhetspolisen arbetar bl.a. för att förhindra att Sverige används som bas för rekrytering, finansiering eller planering av terrordåd, oavsett mot vilket land dessa riktar sig, och för att förebygga att personer med anknytning till terroristnätverk besöker Sverige eller försöker bosätta sig här.

Det internationella samarbetet förutsätter ett ömsesidigt och väl fungerande informationsutbyte. Vad som sägs i avsnitt 7.4 om informationsutbyte vid internationellt samarbete är i allt väsentligt giltigt också för Säkerhetspolisens del. Även Säkerhetspolisen bör få behandla personuppgifter för att fullgöra internationella åtaganden.

Tekniskt biträde

Enligt 3 § första stycket 3 i Säkerhetspolisens instruktion ingår det i Säkerhetspolisens uppgifter att lämna tekniskt biträde åt polisväsendet i den utsträckning som det är lämpligt med hänsyn till verksamhetens art. Säkerhetspolisen har möjlighet att bistå med bl.a. teknisk utrustning som den övriga polisen inte har. Det tekniska biträdet används framför allt vid verkställighet av vissa tvångsmedel. Säkerhetspolisen har nämligen till uppgift att hantera de datasystem som används för att samla in uppgifter från hemlig teleavlyssning och hemlig teleövervakning. Säkerhetspolisen ansvarar för kontakter med operatörerna, när det finns ett domstolsbeslut beträffande tvångsmedel på teleområdet, och tar emot och lagrar den information som operatörerna levererar i enlighet med domstolsbesluten. Detta gäller inte enbart Säkerhetspolisens egna ärenden utan samtliga ärenden av detta slag i landet, oberoende av om förundersökningen bedrivs hos Säkerhetspolisen, inom den övriga polisen, hos Tullverket eller hos Ekobrottsmyndigheten. Behöriga tjänstemän vid polismyndigheterna, och i förekommande fall Tullverket, hämtar in informationen från Säkerhetspolisen och behandlar den vidare. Säkerhetspolisen kan även lämna biträde till den övriga polisen vid hemlig rumsavlyssning. Säkerhetspolisens uppgift som tekniskt biträde är främst en administrativ hantering, men den kräver personuppgiftsbehandling som faller under ändamålet brottsbekämpning. Denna behandling bör nämnas särskilt i den nya lagen.

I datasystemet för hemliga tvångsmedel hanteras också material från hemliga tvångsmedel i ärenden som handläggs av Säkerhetspolisen.

Personuppgiftsbehandlingen i denna del faller under Säkerhetspolisens brottsutredande verksamhet eller, när det gäller hemlig teleavlyssning enligt lagen om särskild utlänningskontroll eller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott, uppgiften att förebygga, förhindra eller upptäcka brott.

Behandling av uppgifter för diarieföring m.m.

På motsvarande sätt som för övriga polisen bör det införas en bestämmelse som gör det möjligt för Säkerhetspolisen att, utan hinder av vad som gäller i övrigt, behandla uppgifter om det är nödvändigt för diarieföring eller för handläggningen av ett ärende eller liknande som kommit in till Säkerhetspolisen. I avsnitt 7.5 behandlas frågan om förhållandet mellan bestämmelserna om diarieföring m.m. och bestämmelserna om gemensamt tillgängliga uppgifter.

16.3.3 Behandling av uppgifter för att tillhandahålla information till andra

Regeringens förslag: Personuppgifter som behandlas i Säkerhetspolisens brottsbekämpande verksamhet ska också få behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. en myndighets verksamhet, om tillhandahållandet sker i syfte att samverka mot brott,
3. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller
4. brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation.

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

Utredningen föreslår inte några särskilda bestämmelser för behandling av uppgifter för att tillhandahålla information till andra.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår emellertid inte någon bestämmelse om behandling av personuppgifter för att tillhandahålla information till annan myndighet i syfte att samverka mot brott.

Remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag när det gäller Säkerhetspolisen.

Skälen för regeringens förslag: Som konstateras i promemorian måste Säkerhetspolisen, i likhet med polisen i övrigt, kunna behandla den information som finns lagrad i digital form för att i viss utsträckning tillhandahålla den till andra brottsbekämpande enheter inom polisen eller till

andra myndigheter. Vad som sägs i avsnitt 7.6 om sekundära ändamål för behandling av personuppgifter har därför giltighet även för Säkerhetspolisens del. Vad som sägs där om tillämpningen av offentlighets- och sekretesslagen gäller också Säkerhetspolisen.

Behovet av informationsutbyte mellan Säkerhetspolisen och andra enheter inom polisväsendet är allmänt sett inte lika framträdande som behovet av informationsutbyte mellan olika enheter inom polisen i övrigt. Detta beror på att den information som Säkerhetspolisen behandlar ofta är av den arten att den varken kan eller bör vidarebefordras. Motsvarande gäller informationsutbyte mellan Säkerhetspolisen och andra brottsbekämpande myndigheter. Det finns emellertid situationer där Säkerhetspolisen kan behöva vidarebefordra information som den har samlat in, exempelvis för att kunna förhindra allvarliga brott som ligger utanför Säkerhetspolisens behörighet. Som exempel kan nämnas att det vid hemlig teleavlyssning som rör spioneri avslöjas konkreta planer på ett förestående bankrån. Den typen av information vidarebefordras normalt till den övriga polisen, i syfte att rånbrottet ska kunna förhindras. Det rör sig här om s.k. överskottsinformation, vars användning regleras i 27 kap. 23 a § rättegångsbalken. Likaså måste Säkerhetspolisen kunna vidarebefordra uppgifter om planerade eller begångna brott riktade mot någon som har personskydd, om det är fråga om ett brott som ligger utanför Säkerhetspolisens ansvarsområde.

Frågan är då om bestämmelsen om de sekundära ändamålen för Säkerhetspolisen ska utformas på samma sätt som för polisen i övrigt. Från brottsbekämpningssynpunkt bör Säkerhetspolisen ha samma möjlighet att lämna uppgifter till andra polisenheter som polisen i övrigt. Likaså har Säkerhetspolisen samma behov av att kunna lämna uppgifter till åklagare som polisen i övrigt, om åklagaren behöver uppgiften för sin verksamhet.

Säkerhetspolisens intresse av att kunna lämna uppgifter till exempelvis Tullverket är mindre tydligt. Ibland kan det emellertid finnas ett samband mellan den brottslighet som Tullverket bekämpar och den brottslighet som hör till Säkerhetspolisens ansvarsområde. Det förekommer t.ex. att narkotikabrottslighet används för att finansiera terroristbrott. Det medför att Säkerhetspolisen kan komma att få del av uppgifter om exempelvis grov narkotikasmuggling. Tullverket har också en viktig roll när det gäller gränskontrollen. I den verksamheten kan Säkerhetspolisen och Tullverket behöva utbyta information t.ex. om personer som anses innebära säkerhetsrisker eller som av annat skäl bör hindras att komma in i landet.

Kustbevakningens uppdrag bl.a. när det gäller gränskontrollen innebär att det kan finnas behov för Säkerhetspolisen att kunna tillhandahålla information också till den myndigheten. Eftersom Skatteverket enbart bedriver förundersökning angående ett fåtal brottstyper som räknas upp i 1 § första stycket lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar kan det förefalla som om behovet av att kunna lämna uppgifter till den verksamheten inte är så stort. I Säkerhetspolisens uppgift att utreda finansiering av allvarlig brottslig verksamhet kan det emellertid finnas behov av att utbyta uppgifter även med Skatteverket.

Som beskrivs i avsnitt 7.6 har regeringen tagit initiativ till en nationell mobilisering mot den grova organiserade brottsligheten. En av de vikti-

gaste åtgärderna är ökad samverkan mellan myndigheter. Inom ramen för den nationella mobiliseringen har Säkerhetspolisen fått i uppdrag av regeringen att ha huvudansvaret för att förebygga, kartlägga och motverka den grova organiserade brottslighetens otillåtna påverkan på viktiga samhällsfunktioner. I uppdraget (dnr Ju2008/5775/PO) ingår bl.a. att bedriva underrättelsearbete i syfte att motverka den grova organiserade brottslighetens otillåtna påverkan på politiker, myndighetsföreträdare och journalister, att delge berörda myndigheter operativ information till stöd för deras arbete mot den grova organiserade brottsligheten samt att ge rådgivning och stöd till såväl polismyndigheter som andra berörda myndigheter när det gäller otillåten påverkan på viktiga samhällsfunktioner. En förutsättning för att Säkerhetspolisen ska kunna fullgöra sitt uppdrag på ett effektivt sätt är att Säkerhetspolisen har möjlighet att tillhandahålla information till andra myndigheter, såväl brottsbekämpande som andra.

Samverkansrådet mot terrorism, som bildades på initiativ av Säkerhetspolisen år 2005, är en struktur för samarbete mellan elva myndigheter för att möta hotet från terrorism. Arbetet i rådet tar sikte på att förebygga, avvärja, skydda mot och hantera frågor rörande terrorism. Inom ramen för detta arbete har flera områden identifierats som viktiga att utveckla. Ett av dessa är möjligheten att delge information, såväl operativ som icke-operativ, mellan myndigheterna i samverkansrådet för att på så sätt öka kunskaperna om terrorism. I rådet ingår såväl brottsbekämpande som andra myndigheter.

Mot bakgrund av detta är det tydligt att Säkerhetspolisen behöver kunna tillhandahålla information till andra myndigheter. Det sekundära ändamålet att kunna tillhandahålla information till andra brottsbekämpande myndigheter bör därför utformas på samma sätt för Säkerhetspolisen som för polisen i övrigt. Vidare bör det, i likhet med vad som föreslås för polisen i övrigt, införas en bestämmelse som ger Säkerhetspolisen möjlighet att behandla personuppgifter om det är nödvändigt för att tillhandahålla information som behövs i andra myndigheters verksamhet, om det sker i syfte att samverka mot brott.

Säkerhetspolisen måste även fortsättningsvis kunna tillhandahålla information till utländska myndigheter som bedriver brottsbekämpande verksamhet eller till mellanfolkliga organisationer med sådana uppgifter.

Säkerhetspolisen har också, på grund av sina speciella uppgifter, behov av att i vissa särskilda fall kunna tillhandahålla information till Försvarsmaktens underrättelseverksamhet och säkerhetstjänst. På samma sätt som brottsbekämpningen i vissa avseenden är en för flera myndigheter gemensam verksamhet är också den underrättelseverksamhet som rör rikets säkerhet en för Säkerhetspolisen och Försvarsmakten gemensam angelägenhet. Det måste därför, som föreslås i promemorian, finnas ett utrymme för att utbyta information mellan myndigheterna, utöver information som syftar till att samverka mot brott.

För att Säkerhetspolisen ska få behandla uppgifter för det nu aktuella ändamålet ska det vara fråga om en uppgift som Säkerhetspolisen bedömer behövs i Försvarsmaktens verksamhet. Härutöver bör det krävas särskilda skäl för att tillhandahålla uppgiften. Härigenom markeras att bestämmelsen ska tillämpas restriktivt. Ett exempel på en situation där den torde kunna tillämpas är att det i Säkerhetspolisens brottsbekämpande verksamhet kommer fram uppgifter som samtidigt har betydelse

för Försvarsmaktens verksamhet. Det kan t.ex. röra sig om för landets säkerhet viktiga uppgifter om en försvarsanställd eller någon i dennes närmaste krets eller om svagheter i skyddet hos någon av Försvarsmaktens anläggningar.

I avsnitt 7.6 föreslås en bestämmelse om behandling av uppgifter för att tillhandahålla information till riksdagen eller regeringen, jfr 10 kap. 15 § offentlighets- och sekretesslagen (2009:400). En motsvarande bestämmelse bör införas för Säkerhetspolisen. Om Säkerhetspolisen har skyldighet att lämna ut uppgifter till någon annan enligt lag eller förordning måste myndigheten också kunna genomföra den behandling som krävs för att fullgöra skyldigheten. Som exempel kan nämnas den lagfästa skyldigheten att underrätta bl.a. anhöriga till en person som har berövats friheten.

När det gäller efterlysta personer och avlägsnanden ur riket föreslås för den övriga polisen en informationsbestämmelse om att regeringen meddelar föreskrifter om att sådana personuppgifter får lämnas till vissa särskilt angivna myndigheter, se avsnitt 7.6. Eftersom Säkerhetspolisen har vissa uppgifter enligt bl.a. lagen om särskild utlänningskontroll bör motsvarande bestämmelse införas för Säkerhetspolisens del.

Det förtjänar att påpekas att ändamålsbestämmelser av det slag som nu föreslås inte reglerar vad som får utlämnas eller hur detta ska ske. Bestämmelserna är inte sekretessbrytande.

16.4 Gemensamt tillgängliga uppgifter

16.4.1 Allmänt om regleringen

Regeringens förslag: Särskilda bestämmelser ska gälla för behandling av uppgifter som görs eller har gjorts gemensamt tillgängliga i Säkerhetspolisens verksamhet. Personuppgifter ska få göras gemensamt tillgängliga i Säkerhetspolisens verksamhet om det behövs för något av de ändamål för vilka behandling får ske inom Säkerhetspolisen. Uppgifter om DNA-profiler får dock inte göras gemensamt tillgängliga.

Bestämmelserna om gemensamt tillgängliga uppgifter ska inte gälla när personuppgifter behandlas med stöd av bestämmelserna om diarieföring m.m.

Utredningen har inte något motsvarande förslag.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian tydliggör dock inte förhållandet mellan bestämmelserna om gemensamt tillgängliga uppgifter och de föreslagna bestämmelserna om behandling av personuppgifter för diarieföring m.m.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget när det gäller Säkerhetspolisen.

Skälen för regeringens förslag: Säkerhetspolisens personuppgiftsbehandling sker i stor utsträckning i gemensamma register, analysdatabaser och ärendehanteringssystem. Oftast innebär en sådan behandling att ett

flertal personer har tillgång till de behandlade uppgifterna. I avsnitt 9 konstateras att ju fler personer som har åtkomst till personuppgifter, desto större är risken för otillbörliga intrång i den personliga integriteten. Av samma skäl som anges där bör det i den nya lagen tas in särskilda bestämmelser för behandlingen av uppgifter som ”görs eller har gjorts gemensamt tillgängliga” i Säkerhetspolisens verksamhet. Vad som avses med ”görs eller har gjorts gemensamt tillgängliga” utvecklas i avsnitt 9.1. Bestämmelserna bör, liksom för polisen i övrigt, innehålla bl.a. krav på särskilda upplysningar, gallring och sökbegränsningar.

För polisen i övrigt föreslås en bestämmelse som begränsar och preciserar vilka personuppgifter som får göras gemensamt tillgängliga. Frågan är om det behövs en motsvarande bestämmelse för Säkerhetspolisen.

Säkerhetspolisen tillämpar bestämmelserna i 33 och 34 §§ polisdatalagen om SÄPO-registret på det centralregister som myndigheten för. En övervägande majoritet av de anteckningar som görs i registret sker på den grunden att det finns särskilda skäl för registreringen med hänsyn till registrets ändamål (33 § första stycket 3 polisdatalagen). Att särskilda skäl används som registreringsgrund i flertalet fall har sin grund i att man i gällande lagstiftning inte har lyckats att precisera de olika kategorier av personuppgifter som Säkerhetspolisen behöver behandla. Den nuvarande lagstiftningen speglar alltså inte det konkreta behovet av behandling av personuppgifter.

Regeringen delar utredningens och promemorians uppfattning att de intressen som Säkerhetspolisen har till uppgift att skydda motiverar att Säkerhetspolisen ges större handlingsfrihet än den övriga polisen i fråga om vilka uppgifter som får behandlas (se bl.a. SOU 1997:65 s. 243). Skälet till detta 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 i underrättelsearbete och renodlat förebyggande arbete.

Verksamhetens särdrag talar för att de begränsningar som föreslagits för polisen i övrigt för att göra uppgifter gemensamt tillgängliga inte bör gälla för Säkerhetspolisen. I samma riktning talar svårigheten att förutse och i lag uttrycka de olika kategorier av personuppgifter som bör få göras gemensamt tillgängliga hos Säkerhetspolisen. Vidare är Säkerhetspolisens verksamhet till sin natur sådan att informationen sprids i mindre utsträckning än inom polisen i övrigt. Därför bör Säkerhetspolisen få göra personuppgifter gemensamt tillgängliga om det behövs för något av de primära ändamål för vilka den får behandla personuppgifter. Undantag bör dock gälla för uppgifter om DNA-profiler. Något behov av att göra sådana uppgifter gemensamt tillgängliga torde inte finnas.

16.4.2 Särskilda upplysningar

Regeringens förslag: Vid behandling av gemensamt tillgängliga uppgifter ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål uppgifterna behandlas.

Om en uppgift direkt kan hänföras till en person som inte är misstänkt vare sig för visst brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det på samma sätt framgå att personen som uppgiften avser inte är misstänkt.

Uppgifter, som avser en person som kan antas ha samband med brottslig verksamhet, ska som regel förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon sådan upplysning behöver dock inte lämnas om det på grund av särskilda omständigheter är onödigt, eller 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 och analysen befinner sig i ett inledande skede.

Utredningen har inte något motsvarande förslag.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna tillstyrker eller har inget att invända mot förslaget.

Skälen för regeringens förslag: Enligt 33 § andra stycket polisdatalagen ska det av SÄPO-registret framgå på vilken grund varje registrering har skett. Säkerhetspolisen har för närvarande inte någon skyldighet att förse personuppgifter med särskilda upplysningar om huruvida en person som behandlas är misstänkt eller inte eller om trovärdigheten hos en uppgiftslämnare. De behandlade uppgifterna förses ändå regelmässigt med sådana upplysningar. Syftet med särskilda upplysningar 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. I avsnitt 10 föreslås att det vid behandling av gemensamt tillgängliga uppgifter hos den övriga polisen ska framgå om en person inte är misstänkt. Vidare ska uppgifter som avser en person som kan antas ha samband med brottslig verksamhet som regel förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av särskilda omständigheter är onödigt.

De skäl som motiverar sådana bestämmelser har giltighet även för den behandling som sker hos Säkerhetspolisen. I likhet med vad som föreslås i promemorian bör därför sådana bestämmelser införas i den nya lagen. Dessa bör dock anpassas till Säkerhetspolisens verksamhet på så sätt att kravet på upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak inte bör gälla upplysningar som har tillförts en uppgiftssamling som har skapats för att bearbeta och analysera information, så länge bearbetningen och analysen befinner sig i ett inledande skede. När arbetet har nått längre, exempelvis när ett underrättelseprojekt inriktat på viss brottslighet har påbörjats, måste dock kravet uppfyllas.

16.4.3 Sökbegränsningar

Regeringens förslag: Känsliga personuppgifter får användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som gäller för Säkerhetspolisens behandling av personuppgifter.

Utredningen lämnar inte något motsvarande förslag.

Remissinstanserna har inte yttrat sig i saken.

Promemorians förslag överensstämmer i huvudsak med regeringens när det gäller användningen av känsliga personuppgifter som sökbegrepp. Därutöver föreslår promemorian bestämmelser om vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Säkerhetspolisen* avstyrker dock förslaget att fri sökning ska vara möjlig endast i en viss handling eller ett visst ärende. Enligt Säkerhetspolisen måste en behörig tjänsteman få söka fritt redan när han eller hon får en träffbild med ett visst antal ärenden. Säkerhetspolisen anser vidare att frågan om vilka databaser som vissa tjänstemän ska få söka fritt i inte bör regleras i lag och pekar på ambitionen att lagstiftningen ska vara teknikneutral. *Riksdagens ombudsmän* ifrågasätter om känsliga personuppgifter bör få användas som sökbegrepp för samtliga de ändamål för vilka Säkerhetspolisen föreslås få behandla personuppgifter.

Skälen för regeringens förslag

Känsliga personuppgifter

Polisdatalagen innehåller inte några bestämmelser om sökbegränsningar. Det innebär att det inte finns några begränsningar i fråga om användning av vissa uppgifter som sökbegrepp. Det enda undantaget kan sägas vara bestämmelsen i 5 § polisdatalagen om behandling av känsliga personuppgifter, men den bestämmelsen gäller behandlingen generellt. I avsnitt 11.2 föreslås att känsliga personuppgifter inte ska få användas som sökbegrepp inom den övriga polisverksamheten. Det innebär exempelvis att uppgifter som avslöjar politisk åsikt eller religiös övertygelse eller som rör hälsa eller sexualliv inte får utgöra sökbegrepp. Frågan är om detsamma bör gälla för Säkerhetspolisen.

I Säkerhetspolisens verksamhet kan uppgifter av de angivna slagen ha stor betydelse. I arbetet med att förebygga och upptäcka terroristbrott kan t.ex. uppgifter om en persons politiska åsikt eller religiösa övertygelse vara viktiga. Vid brott mot rikets säkerhet kan uppgifter av det slaget bidra till att utröna om det finns något motiv för gärningen. Ett totalt förbud mot att använda sådana uppgifter som sökbegrepp skulle därför innebära en risk för att nödvändig analys och bearbetning av information inte kan genomföras. Verksamhetsskäl talar alltså för att man för Säkerhetspolisens del inte bör förbjuda användningen av känsliga personuppgifter som sökbegrepp. Som anförs i promemorian måste emellertid verksamhetsintresset vägas mot intresset av att skydda de personer, vilkas uppgifter behandlas, mot intrång i den personliga integriteten. Huvudregeln bör vara att det är förbjudet att använda känsliga person-

uppgifter som sökbegrepp. Om en sådan användning är absolut nödvändig för något av de ändamål som Säkerhetspolisen får behandla personuppgifter för, bör den dock vara tillåten. Med en sådan regel kan känsliga personuppgifter inte rutinmässigt användas som sökbegrepp utan först sedan det vid en prövning av behovet i det enskilda fallet konstateras att det finns ett påtagligt behov. *Riksdagens ombudsmän* ifrågasätter om känsliga personuppgifter bör få användas som sökbegrepp för samtliga de ändamål för vilka Säkerhetspolisen får behandla personuppgifter. Mot bakgrund av de höga krav som ställs för användningen av känsliga personuppgifter som sökbegrepp torde det vid behandling av personuppgifter inom ramen för vissa delar av Säkerhetspolisens verksamhet knappast bli aktuellt med sådana sökningar, t.ex. vid tekniskt biträde till andra brottsbekämpande myndigheter. Det kan dock inte uteslutas att ett sådant behov någon gång kan föreligga. Möjligheten att använda känsliga personuppgifter som sökbegrepp bör därför inte begränsas att gälla endast för vissa ändamål.

Andra sökbegränsningar

Hos Säkerhetspolisen behandlas ett stort antal kategorier av personuppgifter. I avsnitt 16.4.1 bedöms att det inte är möjligt eller lämpligt att, på samma sätt som för den övriga polisverksamheten, ange vilka olika kategorier av personuppgifter som får göras gemensamt tillgängliga. Av samma skäl bör man inte för Säkerhetspolisen införa det slag av sökbegränsningar som föreslås för polisen i övrigt. Några sådana sökbegränsningar finns inte heller i nuvarande lagstiftning.

I promemorian föreslås att de begränsningar i möjligheterna att göra sökningar som tillämpas av Säkerhetspolisen i centralregistret bör gälla även i fortsättningen. Förslaget avstyrks av *Säkerhetspolisen* som anför att den föreslagna bestämmelsen innebär att den enskilde tjänstemannen får svårt att hitta alternativa sökvägar och i stället måste granska varje ärende i träffbilden för att finna det eller de relevanta ärendena. Ett sådant förfarande är enligt Säkerhetspolisen tidsödande och ineffektivt och kan dessutom leda till att tjänstemannen granskar sådana ärenden som han eller hon egentligen inte har behov av. Säkerhetspolisen framhåller också vikten av att skapa en teknikneutral lagstiftning som tar hänsyn till utvecklingen och anser det olyckligt om den nya lagen utformas med utgångspunkt i dagens tekniska lösningar.

Säkerhetspolisens brottsbekämpning avser särskilt svårupptäckt brottslighet och tyngdpunkten ligger på underrättelsearbete och förebyggande arbete, där informationen inte kan vara lika konkretiserad som när det gäller enskilda brott. Säkerhetspolisen har därför större behov än polisen i övrigt att fritt kunna söka i sin information. De uppgifter som behandlas inom Säkerhetspolisen är som regel av sådan karaktär att de inte sprids inom myndigheten i samma utsträckning som uppgifter inom polisen i övrigt. Generellt sett är också tillgången till uppgifter mera begränsad hos Säkerhetspolisen än hos den övriga polisen och styrs i större utsträckning av den enskilde tjänstemannens behörighet. Sökbegränsningar som tar sin utgångspunkt i nuvarande system riskerar att motverka syftena med den nya lagen, samtidigt som teknikutvecklingen kan komma

att hämmas. Detta motiverar att det inte införs några särskilda sökbegränsningar för Säkerhetspolisen i den nya lagen, med undantag för användandet av känsliga personuppgifter som sökbegrepp. Regeringen eller den myndighet regeringen bestämmer har dock möjlighet att meddela föreskrifter om sökbegränsningar. Om det exempelvis vid tillsynen över Säkerhetspolisens personuppgiftsbehandling visar sig finnas behov av sökbegränsningar kan alltså föreskrifter om sådana meddelas.

16.4.4 Bevarande och gallring

Regeringens förslag: Personuppgifter som har gjorts gemensamt tillgängliga ska 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.

Säkerhetspolisen får, om det finns särskilda skäl, besluta att personuppgifter får behandlas längre tid än vad som nu har sagts, om uppgifterna fortfarande behövs för det ändamål som de behandlas för. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, i fråga om uppgifter i en uppgiftssamling som skapats för att bearbeta och analysera information, senast vid utgången av det tredje kalenderåret efter beslutet.

Regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att uppgifter, trots bestämmelser om gallring, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Bestämmelserna om gallring ska inte tillämpas på uppgifter i ärenden om utredning eller beivrande av brott. För behandling av sådana uppgifter ska samma bestämmelser gälla som i den övriga polisens verksamhet.

Utredningen föreslår inte några särskilda regler om gallring för Säkerhetspolisens verksamhet. Den allmänna bestämmelsen, att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, föreslås gälla.

Remissinstanserna har inte yttrat sig i frågan.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inget att invända mot promemorians förslag. *Justitiekanslern* framhåller dock vikten av att gallring sker inom rimlig tid och föreslår bl.a. att man i det fortsatta arbetet överväger kortare gallringsfrister för vissa personuppgifter.

Skälen för regeringens förslag: De allmänna utgångspunkter för bevarande och gallring som föreslås gälla för övriga polisen bör som tidigare nämnts gälla i tillämpliga delar för Säkerhetspolisen. Uppgifter i ärenden om utredning eller beivrande av brott bör inte omfattas av lagens gallringsbestämmelser. När sådana uppgifter har gjorts gemensamt till-

gängliga bör det dock hos Säkerhetspolisen på samma sätt som för övriga polisen gälla begränsningar i möjligheten att behandla uppgifterna (se avsnitt 14.4).

När det gäller övriga uppgifter som har gjorts gemensamt tillgängliga bör dessa, på samma sätt som motsvarande uppgifter hos den övriga polisen, omfattas av särskilda gallringsbestämmelser. Utgångspunkten för dessa gallringsbestämmelser bör vara att samma regler ska tillämpas, oavsett var i Säkerhetspolisens verksamhet uppgiften behandlas. Det bör alltså, som huvudregel, inte gälla olika gallringsfrister beroende på i vilken uppgiftssamling uppgiften förekommer. Gallringsbestämmelserna bör anpassas till Säkerhetspolisens särskilda verksamhet. Den nuvarande bestämmelsen om gallring av uppgifter i SÄPO-registret (35 § polisdatalagen) bör tas som utgångspunkt. Där föreskrivs att uppgifter ska gallras senast tio år efter det att en sådan uppgift om personen som kan föranleda registrering senast infördes.

Flera omständigheter talar för att gallringsfristerna för Säkerhetspolisen bör vara förhållandevis korta. Uppgifter som behandlas av Säkerhetspolisen är till sin natur ofta särskilt känsliga ur integritetssynpunkt. Mängden av känsliga uppgifter torde också, allmänt sett, vara förhållandevis större hos Säkerhetspolisen än hos polisen i övrigt. Det finns dock omständigheter som talar i motsatt riktning. I den speciella verksamhet som Säkerhetspolisen bedriver kan det ofta vara nödvändigt att bevara uppgifter under längre tid än inom polisen i övrigt. Som exempel kan nämnas att främmande agenter kan befinna sig länge i ett land innan de påbörjar verksamhet som är brottslig. Det kan exempelvis vara nödvändigt att kontrollera och följa personer under en betydligt längre tid när misstanken avser brottslig verksamhet riktad mot rikets säkerhet än vad som är sakligt motiverat när det gäller brottslig verksamhet av annat slag. Vidare har flertalet av de brott som Säkerhetspolisen bekämpar en straffskala som innebär att brotten preskriberas först efter lång tid.

Promemorians slutsats att en allmän gallringsfrist om, som längst, tio år utgör en lämplig avvägning mellan verksamhetens behov och den enskildes krav på att uppgifter inte ska bevaras alltför lång tid är enligt regeringens mening rimlig. Huvudregeln bör därför vara att uppgifter i Säkerhetspolisens verksamhet ska gallras inom tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. I fråga om vissa personuppgifter bör det dock gälla en kortare gallringsfrist. Personuppgifter som förekommer i en uppgiftssamling som skapats för att bearbeta och analysera information bör sålunda gallras tidigare, lämpligen inom tre år efter det kalenderår då den senaste registreringen avseende personen gjordes.

Det bör framhållas att de gallringsbestämmelser som föreslås avser den senaste tidpunkt när uppgifterna måste gallras. Om det redan före gallringstidens utgång står klart att uppgifterna saknar betydelse för Säkerhetspolisens brottsbekämpande verksamhet ska de gallras redan då.

Den nuvarande gallringsregeln för SÄPO-registret medger att uppgifter bevaras även sedan tioårsfristen har löpt ut, om det finns särskilda skäl. Vad som är särskilda skäl utvecklas inte närmare i förarbetena. Det finns inte heller någon regel som anger vid vilken tidpunkt uppgifterna då ska gallras. I promemorian föreslås att det i den nya lagen införs en motsvarande möjlighet till förlängning av gallringsfristen. *Justitiekanslern* anför

att en sådan bestämmelse som föreslås i promemorian i praktiken innebär att Säkerhetspolisen får behandla gemensamt tillgängliga personuppgifter under i stort sett obegränsad tid. Som framhålls i promemorian kan en tioårig gallringsfrist i vissa fall vara alltför kort, varför det även i fortsättningen bör finnas en möjlighet att i enskilda fall bevara uppgifterna längre. Av integritetsskäl bör dock möjligheten till förlängning av gallringsfristen snävas in i förhållande till nuvarande reglering. Det bör för det första, liksom nu, krävas särskilda skäl för att kunna förlänga gallringsfristen. Ett särskilt skäl kan vara att ärendet rör en företeelse eller en person som kan antas få ny aktualitet. Varje avsteg från den normala gallringsfristen bör vidare dokumenteras i ett särskilt beslut, där behovet av längre tids bevarande motiveras. Dessutom bör beslut av detta slag vara tidsbegränsade. Härigenom säkerställs att gallringsfristerna inte rutinmässigt förlängs. En särskild regel som innebär att Säkerhetspolisen ska kunna fatta beslut om bevarande under viss ytterligare tid bör således införas. Den tiden bör inte kunna vara längre än den ursprungliga tiden för bevarande.

Liksom enligt gällande rätt bör regeringen eller den myndighet som regeringen bestämmer ha möjlighet att meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

17 Informationssäkerhet och tillsyn m.m.

17.1 Säkerheten vid behandling av uppgifter

I takt med att polisen utvecklar nya IT-lösningar måste man också utveckla rutinerna för dataskydd och säkerheten vid behandlingen. Om allmänheten ska ha förtroende för den informationsbehandling som sker hos polisen så krävs det nämligen inte bara en modern lagstiftning. Polisen måste också aktivt verka för att den tillämpas på avsett sätt. Detta gäller både när man bygger nytt IT-stöd, i förvaltningen av befintliga system och i den dagliga användningen av olika IT-system. Det åligger också polisen att följa upp att lagstiftningen tillämpas med respekt för enskildas integritet. Slutligen måste det finnas god säkerhet mot externa försök att komma åt eller påverka informationen.

Polisen eftersträvar hög informationssäkerhet eftersom information är ett av polisens viktigaste arbetsredskap. I takt med att den elektroniska informationshanteringen ökar ställs högre krav på IT-säkerheten. Polisen arbetar med en ny plan för informationssäkerhet som planeras vara genomförd vid utgången av år 2012.

När det gäller skyddet mot externa angrepp har polisen generellt sett ett väl utbyggt system för tillträdesskydd och fysisk kontroll. Man har också brandväggar mot extern kommunikation och eget separat nätverk. Vidare används kryptering för viss kommunikation.

Den interna kontrollen är under vidareutveckling. Den omfattar bl.a. interna säkerhetsrutiner, rutiner för behörighet och åtkomstkontroll samt loggning av genomförda åtgärder.

Ju mer omfattande ett informationssystem är och ju känsligare uppgifter det innehåller, desto viktigare är det att det finns olika behörighetsni-

våer för skilda kategorier av uppgifter och användare. Den nya lagstiftningen ställer större krav än tidigare på att polisen genom tekniska åtgärder begränsar den enskilde tjänstemannens tillgång till information till det han eller hon behöver för att fullgöra sina arbetsuppgifter. För den interna kontrollen finns redan system för autenticiering, dvs. kontroll av användarens identitet, men systemet kommer att utvecklas ytterligare i samband med att polisen successivt tar ett nytt loggningssystem i bruk. Syftet är att polisen ska kunna försäkra sig om att varje användare får del endast av de uppgifter han eller hon behöver för sitt arbete. De åtgärder som en person vidtar noteras i polisens loggningssystem. Därmed kan man i efterhand kontrollera användningen.

Polisen har utvecklat ett helt nytt system som förbättrar den tekniska kontrollen över IT-användningen benämnt polisens centrala säkerhetslogg (CSL). CSL innebär att man går över från manuell logghantering för enskilda datasystem till ett enda centralt loggningssystem med hög inbyggd säkerhet. Det övergripande syftet med CSL är dels att skydda enskildas integritet, dels att skydda den information som polisen behandlar mot otillåten behandling och angrepp. Tanken är att CSL ska logga all behandling som sker i polisens datasystem. Genom automatisk analys av inkomna loggar ska polisen kunna följa upp och kontrollera dataanvändningen på ett mera systematiskt sätt. Systemet ska slå larm vid felaktig eller obehörig hantering, t.ex. obehörig inloggning. CSL tas från sommaren 2009 successivt i bruk för befintliga system. Avsikten är att det ska byggas in i nya system.

Tekniska åtgärder är emellertid bara en del av säkerheten. Det är enligt regeringens mening också viktigt att polisen noga kontrollerar och följer upp tilldelningen av behörigheter. Den nya lagen ställer högre krav än tidigare i detta avseende.

En annan viktig säkerhetsaspekt är personalens medvetenhet om riskerna för angrepp mot datasystemen och behovet av att kvalitetssäkra informationen. Polisen måste försäkra sig om att personalen har den utbildning som krävs för att garantera dataskydd och informationssäkerhet. Även detta ingår i polisens plan för att öka informationssäkerheten.

En viktig aspekt för den enskilde när det gäller dataskydd är krav på att de uppgifter som behandlas ska vara aktuella och adekvata, dvs. hålla hög kvalitet. Med stora uppgiftsmängder följer en ökad risk att informationen inte blir så användbar, eftersom uppgifterna kan vara inaktuella eller irrelevanta. Den nya lagstiftningen detaljreglerar inte polisens personuppgiftsbehandling men ställer i gengäld högre krav på systematik och tydlighet vid behandlingen. I kvalitetskontrollen bör också ingå lämpliga tekniska lösningar för att kunna i efterhand kontrollera vem som har fört in eller bearbetat en viss uppgift och möjlighet att spåra sådana åtgärder. Som framgått ovan har polisen nyligen tagit i bruk ett nytt system för sådan kontroll. Härigenom skapas också ett skydd mot att informationen utsätts för interna angrepp.

I andra lagstiftningsärenden har man konstaterat att riktlinjer för informationssäkerhetsarbetet inte bör ges i lag utan vid behov bör ges på lägre föreskriftsnivå (se t.ex. prop. 2007/08:126 s. 149). Enligt regeringens mening behövs inga särskilda bestämmelser om informationssäkerhet i den nya lagen, utöver personuppgiftslagens regler om säkerheten vid

behandlingen, som ska gälla i polisens brottsbekämpande verksamhet på samma sätt som nu (avsnitt 6.4.2).

Polisen bör också, som *Säkerhetspolisen* påpekar, vinnlägga sig om att genomföra säkerhetsanalys samt att analysera och klassificera de uppgifter som förekommer i IT-systemen, i syfte att förbättra informationssäkerheten. Sådan analys bör utgöra en integrerad del av arbetet både vid tillskapandet av nya system och förvaltningen av befintliga.

17.2 Tillsyn

Regeringens förslag: Datainspektionen, som är tillsynsmyndighet enligt personuppgiftslagen, ska utöva tillsyn över polisens behandling av personuppgifter inom den brottsbekämpande verksamheten. Personuppgiftsbehandlingen ska också stå under tillsyn av Säkerhets- och integritetsskyddsnämnden.

Utredningens förslag överensstämmer i huvudsak med promemorians. Utredningen föreslår dock inte att personuppgiftsbehandlingen också ska granskas av Säkerhets- och integritetsskyddsnämnden.

Remissinstanserna har inte haft någon invändning mot utredningens förslag eller har inte kommenterat saken närmare.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* tillstyrker förslaget men anser att det bör klargöras i vad mån nämnden ska vara skyldig att på begäran av en enskild kontrollera om han eller hon varit föremål för personuppgiftsbehandling. *Datainspektionen* anser att det av principiella skäl bör undvikas att två myndigheter parallellt utövar tillsyn över samma verksamhet och att Säkerhets- och integritetsskyddsnämnden inte bör ges en vidare tillsyn än den som nämnden redan har. Datainspektionen är i övrigt positiv till förslaget. Övriga remissinstanser tillstyrker eller har inte något att invända mot förslaget.

Skälen för regeringens förslag

Behovet av fristående tillsynsorgan

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen med uppgift att bl.a. verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter (1 och 2 §§ förordningen [1998:1192] med instruktion för Datainspektionen och 2 § personuppgiftsförordningen [1998:1191]). Denna tillsyn omfattar även den behandling av personuppgifter som sker med stöd av polisdatalagen. Därutöver har Säkerhets- och integritetsskyddsnämnden till uppgift att granska Säkerhetspolisens behandling av uppgifter enligt polisdatalagen, särskilt med avseende på behandlingen av känsliga personuppgifter (1 § andra stycket lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Det kan tilläggas att det ingår i Säkerhets- och integritetsskyddsnämndens uppgifter att på begäran av en enskild kontrollera bl.a. om han eller hon har varit föremål för otillåten personuppgiftsbehandling

hos Säkerhetspolisen. Nämnden är skyldig att utföra kontrollen och att underrätta den enskilde som begärt kontrollen om att den har utförts. En motsvarande ordning finns i ett flertal andra länder. Ett huvudskäl till att Säkerhets- och integritetsskyddsnämnden inrättades, hur tillsynsuppgiften utformades och att nämnden ålades att överlämna resultatet av sin tillsyn till andra myndigheter för åtgärd är att Europadomstolen den 6 juni 2006 i målet Segerstedt–Wiberg m.fl. mot Sverige fann att i fråga om Säkerhetspolisens registrering så uppfyllde varken Riksdagens ombudsmän, Justitiekanslern, den dåvarande Registernämnden eller Datainspektionen, ens sammantagna, kravet på effektiva rättsmedel enligt artikel 13 i Europakonventionen.

Såväl Säkerhetspolisen som polisen i övrigt ska säkerställa att det finns interna funktioner för att kontrollera att myndighetens tjänstemän följer reglerna för personuppgiftsbehandling. Frågan om hur enskilda tjänstemäns tillgång till personuppgifter ska begränsas diskuteras i avsnitt 6.6.

Det är dock inte alltid lätt för en brottsbekämpande myndighet – för vilken det brottsbekämpande arbetet står i fokus – att göra de ofta grannlaga avvägningar mellan brottsbekämpningsintresset och integritetsintresset som är nödvändiga. Det är mot den bakgrunden angeläget att personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet blir föremål för tillsyn av ett i förhållande till polisen fristående organ. I sammanhanget är det viktigt att påpeka att det till stor del gäller sekretess i verksamheten. Det får till följd att den enskilde i många fall inte kommer att kunna ges information om pågående personuppgiftsbehandling som rör honom eller henne och därmed inte heller kommer att ha några praktiska möjligheter att själv göra gällande rätten till exempelvis rättelse eller skadestånd. De brister i skyddet för den enskilde som detta medför kan kompenseras genom ett fristående tillsynsorgan, som har tillgång till sekretesskyddad information. Genom tillsyn av ett fristående organ kan risken för onödiga integritetsintrång minimeras. Dataskyddsrambeslutet (avsnitt 4.4.1) förutsätter att det finns ett fristående tillsynsorgan.

Parallell tillsyn?

Frågan är nu hur denna tillsyn bör anordnas. En möjlighet är att anförtro tillsynen i dess helhet åt Datainspektionen. En sådan lösning skulle innebära en begränsning vad gäller tillsynen över Säkerhetspolisens personuppgiftsbehandling. En annan möjlighet är att överlåta hela tillsynen till ett fristående organ som är särskilt inriktat på att granska brottsbekämpande verksamhet. En tredje möjlighet är att – med vad som gäller i fråga om personuppgiftsbehandling inom Säkerhetspolisen som förebild – anförtro tillsynsuppgifterna åt två olika myndigheter som båda har den nödvändiga fristående rollen, i detta fall dels Datainspektionen, dels en myndighet vars verksamhet är inriktad på granskning av brottsbekämpande verksamhet.

Det finns skäl som talar för att all tillsyn över myndigheternas personuppgiftsbehandling bör ligga på en enda myndighet. Det står då klart vilken myndighet som bär ansvaret för att tillsynen är effektiv. *Datainspektionen* anser att man av principiella skäl bör undvika att två myndigheter parallellt utövar tillsyn över samma verksamhet, eftersom det finns

risk för att en sådan lösning kan leda till oklarheter för allmänheten, tillsynsobjektet och tillsynsmyndigheterna.

Det finns emellertid även fördelar med en ordning där två myndigheter, var och en med utgångspunkt i sitt uppdrag, utövar tillsyn över personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet. Inom Datainspektionen finns det en väl upparbetad kompetens och erfarenhet vad gäller personuppgifts- och integritetsfrågor. En tillsyn genom Datainspektionen ger därför goda förutsättningar att framför allt kontrollera att allmänna principer för behandling av personuppgifter tillämpas också inom den brottsbekämpande verksamheten. Datainspektionen ställer sig också positiv till att myndigheten ges ansvaret för en sådan tillsyn. Samtidigt kan man utgå ifrån att ju större insikt i och erfarenhet av den granskade verksamheten som tillsynsmyndigheten har, desto lättare kan tillsynen inriktas på de områden som kan ge upphov till särskilda risker från integritetssynpunkt. I sammanhanget måste också beaktas att Datainspektionens tillsynsområde är omfattande. I det perspektivet är det av värde om Datainspektionens tillsyn kan kompletteras med tillsyn genom en myndighet som har till särskild uppgift att utöva tillsyn över brottsbekämpande verksamhet. En sådan ”dubbel” tillsyn förekommer, som nyss har nämnts, redan nu, när det gäller behandling av personuppgifter i Säkerhetspolisens verksamhet.

På försvarsunderrättelseområdet gäller också sedan länge en liknande ordning; jfr propositionen Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (prop. 2006/07:46). Tillsynen över Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling utövas dels av Datainspektionen, dels av Försvarets underrättelsenämnd.

Övervägande skäl talar enligt regeringens mening för att välja den sist diskuterade lösningen. Den personuppgiftsbehandling som förekommer i polisens brottsbekämpande verksamhet bör således stå under tillsyn av både Datainspektionen och en annan fristående myndighet, inriktad på tillsyn över brottsbekämpande verksamhet. Säkerhets- och integritetsskyddsnämnden är en sådan myndighet, men dess tillsyn är begränsad till personuppgiftsbehandling på Säkerhetspolisens område. Vidare har nämnden till uppgift att utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel samt kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. Säkerhets- och integritetsskyddsnämnden bör anförtros uppgiften att utöva ytterligare tillsyn över personuppgiftsbehandlingen inom polisen. Tillsynen bör avse personuppgiftsbehandlingen i den brottsbekämpande verksamheten inom hela polisväsendet, inklusive Säkerhetspolisen, och den polisiära verksamheten vid Ekobrottsmyndigheten. Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden ska alltså utöva tillsyn.

Utöver den tillsyn som enligt förslaget ska utövas av Datainspektionen och Säkerhets- och integritetsskyddsnämnden, har både Justitiekanslern och Riksdagens ombudsmän rätt att, i enlighet med sina instruktioner, utöva tillsyn över polisverksamheten. I samband därmed kan de givetvis även kontrollera personuppgiftsbehandlingen vid den aktuella myndigheten.

Vilka uppgifter bör myndigheterna ha?

Det kan först konstateras att personuppgiftslagen tillägger tillsynsmyndigheten, dvs. Datainspektionen, vissa särskilda befogenheter, avsedda att möjliggöra en granskning av om personuppgiftsbehandlingen är laglig. Myndigheten har rätt att på begäran få tillgång till de personuppgifter som behandlas, upplysning om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (43 § personuppgiftslagen). Om Datainspektionen efter en sådan begäran inte kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får myndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem (44 §). Konstaterar Datainspektionen att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt, eller är saken brådskande, får Datainspektionen vid vite förbjuda den personuppgiftsansvarige att fortsätta behandlingen på annat sätt än genom lagring av uppgifterna (45 §). Vidare får Datainspektionen hos länsrätten ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska förstöras. Beslut om utplånande ska dock inte meddelas om det är oskäligt.

Det är naturligt att Datainspektionen har motsvarande uppgifter och befogenheter när den utövar tillsyn över polisens personuppgiftsbehandling. Den nya lagen bör därför innehålla bestämmelser som i allt väsentligt motsvarar de nyss angivna bestämmelserna i personuppgiftslagen. Därmed kommer innehållet i inspektionens tillsyn att bli i stort sett detsamma, oavsett om tillsynen avser personuppgiftsbehandling i polisens brottsbekämpande verksamhet eller personuppgiftsbehandling i annan polisiär verksamhet. Dock bör, av de skäl som anges i avsnitt 6.4.2, Datainspektionen inte ha möjlighet att förena ett förbud mot viss personuppgiftsbehandling med vite.

Säkerhets- och integritetsskyddsnämnden utövar sin tillsyn genom inspektioner och andra undersökningar för att säkerställa att den verksamhet som står under nämndens tillsyn bedrivs på ett författningsenligt sätt. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i regelverket avhjälps (1–2 §§ lagen om tillsyn över viss brottsbekämpande verksamhet). Vidare är nämnden skyldig att på begäran av en enskild person kontrollera om denne har utsatts för ett hemligt tvångsmedel eller, i fråga om Säkerhetspolisen, personuppgiftsbehandling i strid med författningar. Nämnden ska underrätta den enskilde om att kontrollen har utförts (3 §). I sin tillsyn har nämnden rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Också domstolar och förvaltningsmyndigheter som inte omfattas av nämndens tillsyn är skyldiga att lämna nämnden de uppgifter som den behöver (4 §).

Säkerhets- och integritetsskyddsnämndens tillsyn bör, liksom Datainspektionens tillsyn, avse frågan om personuppgiftsbehandlingen står i överensstämmelse med lag och annan författning och inriktas på att människor skyddas mot att deras integritet kränks vid behandlingen.

Säkerhets- och integritetsskyddsnämnden tillstyrker att dess tillsynsuppgift utvidgas i enlighet med förslaget. Nämnden anser att tyngdpunkten i tillsynen bör ligga på den personuppgiftsbehandling som är undandragen allmänhetens insyn och förordar att det klargörs i vad mån nämnden ska vara skyldig att på begäran av en enskild kontrollera om han eller hon varit föremål för personuppgiftsbehandling. Som föreslås i promemorian bör Säkerhets- och integritetsskyddsnämnden tillämpa samma arbetssätt som i sin övriga tillsynsverksamhet. Det innebär att nämnden på eget initiativ eller på enskildas begäran bör kunna genomföra olika slag av inspektioner och utredningar och därvid uttala sig om huruvida det har förekommit felaktigheter vid personuppgiftsbehandlingen. Behovet av inspektioner och kontroller genom nämndens försorg i anledning av en begäran från allmänheten torde vara störst när det gäller personuppgiftsbehandling i sekretesskyddad verksamhet. Skyldigheten att genomföra kontroller på begäran av enskilda bör emellertid gälla all personuppgiftsbehandling i polisens brottsbekämpande verksamhet. Vid sin tillsyn bör nämnden, liksom nu, ha rätt att få tillgång till de upplysningar och det biträde som den begär. Det har inte framkommit något behov av att ge nämnden möjlighet att meddela förelägganden eller förbud eller att ge den möjlighet att föra talan i domstol. Det är lämpligare att nämnden, även fortsättningsvis, om den finner omständigheter som Datainspektionen bör uppmärksammas på, anmäler detta till inspektionen (22 § förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden).

Samråd med Datainspektionen?

En annan fråga, som hör samman med tillsynen, är om det bör införas en skyldighet för polisen att samråda med Datainspektionen i vissa fall. För närvarande finns det en bestämmelse om förhandskontroll i 2 § polisdataförordningen (1999:81). Den innebär att vissa typer av behandling av personuppgifter alltid ska anmälas tre veckor i förväg. Fördelen med en bestämmelse om förhandskontroll eller samrådsskyldighet är att tillsynsmyndigheten informeras om nya behandlingar av personuppgifter och vid behov kan reagera över den planerade behandlingen. Den nuvarande bestämmelsen om förhandskontroll har dock den svagheten att det i praktiken är svårt för Datainspektionen att påverka framtida behandlingar, eftersom anmälan inte behöver göras förrän omedelbart inför igångsättandet av en ny behandling av personuppgifter. Som promemorian föreslår bör det i stället finnas en skyldighet för polisen att i vissa situationer samråda med Datainspektionen, exempelvis när polisen planerar att ta nya större system i bruk, förbereder omfattande förändringar i befintliga system eller genomför förändringar som påverkar hanteringen av särskilt känsliga uppgifter. Som *Datainspektionen* anför innebär en sådan ordning att frågan om integritetsskydd på ett bättre sätt kan beaktas då den väcks på ett tidigt stadium av systemutvecklingsprocessen. Detta är emellertid en fråga som inte bör regleras i lag utan som regeringen kan meddela föreskrifter om.

17.3 Utvärdering

Den föreslagna lagstiftningen innebär att polisens möjligheter att behandla personuppgifter förändras. Den nya lagen ger ramarna för behandlingen utan att styra den i detalj. Reformer av detta slag bör följas upp både när det gäller själva genomförandet och utvecklingen i fråga om tillämpningen av den nya lagstiftningen. Det är också viktigt att identifiera eventuella brister i regleringen. Likaså är det angeläget att ta till vara de synpunkter som den förstärkta tillsynen kan resultera i. Regeringen har genom uppdraget till Rikspolisstyrelsen (se avsnitt 3), som löper fram till dess att lagstiftningen träder i kraft och ska redovisas inom tre månader därefter, försäkrat sig om att kunna följa genomförandet. På sikt bör en utvärdering av reformen göras, men det finns inte skäl att redan nu binda sig för vilka former eller vilket innehåll denna utvärdering bör ha.

18 Ikraftträdande och övergångsbestämmelser

Regeringens förslag: Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ska träda i kraft den 1 mars 2012, då polisdatalagen (1998:622) ska upphöra att gälla.

Fram till utgången av år 2014 ska polisdatalagens bestämmelser tillämpas på behandlingen av personuppgifter i de särskilda undersökningar som har beslutats före ikraftträdandet.

Vissa bestämmelser i den nya lagen om särskilda upplysningar, sökning samt behandling av uppgifter i brottsanmälningar och avslutade förundersökningar behöver inte tillämpas före utgången av år 2014.

Signalements- och kännetecknsregistret och det centrala brottsspaningsregistret, som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av Datainspektionens tillstånd och den upphävda datalagen, får fortsätta att föras enligt nu gällande regler fram till utgången av år 2014. Ett tillstånd från Datainspektionen kan upphöra att gälla tidigare, om registret avanmäls.

Datainspektionens tillstånd för övriga register som enligt polisdatalagens övergångsbestämmelser förs med stöd av datalagen upphör att gälla när den nya lagen träder i kraft.

Utredningen anser det viktigt att tiden fram till dess att den nya regleringen börjar gälla inte blir längre än nödvändigt.

Remissinstanserna har inte haft några synpunkter.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian föreslår dock en kortare övergångsreglering.

Remissinstanserna: *Rikspolisstyrelsen* framhåller behovet av en lång övergångsperiod för att undvika att polisen tvingas lägga resurser på att anpassa äldre datasystem till den nya regleringen i stället för att utveckla nya. Alltför snäva övergångsbestämmelser riskerar enligt styrelsen att leda till att den positiva utveckling som påbörjats vad gäller polisens elektroniska informationshantering bromsas upp. *Åklagarmyndigheten* och *Ekobrottsmyndigheten* framhåller att ikraftträdande- och övergångs-

bestämmelserna bör utformas med beaktande av det arbete som pågår inom Rådet för rättsväsendets informationsförsörjning. För det fall punkten två i övergångsbestämmelserna till polisdatalagen skulle behöva förlängas ytterligare anser *Datainspektionen* att detta inte bör göras generellt utan endast för vissa register.

Skälen för regeringens förslag

Behovet av en övergångsperiod

Rikspolisstyrelsen anför i sitt remissvar att en så kort övergångsperiod som föreslås i promemorian kan leda till avsevärda kostnader för att anpassa polisens befintliga system till den nya regleringen och att kostnaderna beror på hur många av systemen som behöver anpassas. Bland annat mot denna bakgrund gav regeringen i januari 2009 Rikspolisstyrelsen i uppdrag att inventera de datasystem som helt eller delvis förs med stöd av polisdatalagen eller dess övergångsbestämmelser och som omfattas av förslagen i departementspromemorian samt att redovisa vilka av dessa som inte utan förändringar skulle kunna föras med stöd av förslagen. I redovisningen av uppdraget vidhåller Rikspolisstyrelsen behovet av en längre övergångsperiod och pekar på intressemotsättningen, resursmässigt och verksamhetsmässigt, mellan å ena sidan att utveckla nya datasystem samtidigt som man å andra sidan, till ganska betydande kostnader, ska förvalta och lagstiftningsanpassa befintliga system.

När ny lagstiftning beslutas som påverkar förutsättningarna för att skapa tekniska system, behövs i allmänhet en övergångsreglering. Även om polisen har påbörjat arbetet med att modernisera sina datasystem är det först när den nya lagen har beslutats som polisen slutligt kan ta ställning till behovet av nya system och förutsättningarna för att ändra befintliga. Att planera och utveckla datasystem tar tid. Av Rikspolisstyrelsens redovisning framgår att polisen bedömer att flera av de nuvarande systemen kommer att behållas, i vart fall under en tid, och att den nya lagen kommer att kräva anpassning av systemen. Kostnader för att anpassa äldre datasystem som på sikt ska avvecklas bör i möjlig mån undvikas. Hänsyn bör tas till detta när övergångsregleringen utformas. Dessutom behöver polisen tid att förbereda sig på en övergång till den nya regleringen genom utbildning m.m.

En adekvat övergångsreglering åstadkoms dels genom att låta den nya lagen träda i kraft först några år efter det att lagen beslutats, dels genom ett mindre antal preciserade övergångsbestämmelser. Genom att låta lagen träda i kraft först en viss tid efter att den har beslutats undviks omfattande och detaljerade övergångsbestämmelser som riskerar att skapa problem vid tillämpningen. Dessutom ges polisen nödvändig tid att förbereda de åtgärder som krävs. Dessa fördelar överväger de nackdelar som det generellt sett innebär att skjuta på en lags ikraftträdande, exempelvis risken att det efter beslutet men innan ikraftträdandet inträffar något som gör att den nya lagen behöver ändras.

Övergångsbestämmelser

För närvarande sker polisens behandling av personuppgifter dels med stöd av särskilda bestämmelser i polisdatalagen, dels med stöd av den upphävda datalagen och tillstånd från Datainspektionen enligt övergångsbestämmelserna till polisdatalagen, dels med stöd av de allmänna bestämmelserna i polisdatalagen och personuppgiftslagen (se avsnitt 5).

I fråga om den behandling som sker med stöd av särskilda bestämmelser i polisdatalagen, bör det införas övergångsbestämmelser för den behandling som sker i särskilda undersökningar (14 och 15 §§ polisdatalagen). Vissa av dessa undersökningar kommer att omfattas av de föreslagna bestämmelserna om behandling av gemensamt tillgängliga uppgifter, bl.a. bestämmelserna om gallring och särskilda upplysningar. För att undvika att belasta underrättelseverksamheten med arbetet att anpassa pågående särskilda undersökningar till den nya regleringen, bör nuvarande regler under en övergångsperiod fortsätta att tillämpas på de särskilda undersökningar som har påbörjats före lagens ikraftträdande. Övergångstiden bör gälla till utgången av år 2014. En särskild undersökning ska pågå högst ett år (se 16 § polisdatalagen), med möjlighet till fortsatt behandling om det finns särskilda skäl. De flesta särskilda undersökningar bör alltså hinna avvecklas redan innan lagen har trätt i kraft.

Vid övrig behandling av personuppgifter är det framför allt några bestämmelser i den nya lagen som polisen kan få svårigheter att tillämpa redan vid ikraftträdandet. Detta bekräftas i huvudsak av Rikspolisstyrelsen i redovisningen av uppdraget. Det rör sig om delar av regleringen angående gemensamt tillgängliga uppgifter, nämligen vissa av bestämmelserna om särskilda upplysningar, sökbegränsningar samt om behandling av uppgifter i brottsanmälningar och avslutade förundersökningar.

Gemensamt för dessa bestämmelser är att de förutsätter en återkoppling till polisen från åklagarväsendet när en åklagarledd förundersökning eller ett åtal har lagts ned och från domstol om lagakraftvunna domar. Som Rikspolisstyrelsen påtalar saknas det för närvarande sådana rutiner för återkoppling. Det behövs därför övergångsbestämmelser som under en tid medger undantag från tillämpningen av de aktuella bestämmelserna. Rådet för rättsväsendets informationsförsörjning bedriver arbete som bl.a. syftar till att åstadkomma en rutin för elektronisk återkoppling till polisen av beslut av myndigheter i senare led i rättskedjan. *Åklagarmyndigheten* och *Ekobrottsmyndigheten* framhåller vikten av att ikraftträdande- och övergångsbestämmelserna utformas med beaktande av det arbete som pågår.

I fråga om bestämmelserna om sökning är det inte enbart bristen på återkoppling som motiverar övergångsbestämmelser. Bestämmelserna om sökbegränsningar har ingen motsvarighet i gällande reglering och det är enligt *Rikspolisstyrelsen* svårt att hinna åstadkomma nödvändiga anpassningar av nuvarande system före lagens ikraftträdande. Vad gäller kravet på att det ska framgå att en person inte är misstänkt, finns det inte skäl att föreskriva om undantag från tillämpningen i polisens underrättelseverksamhet, eftersom liknande bestämmelser finns i 14 och 19 §§ polisdatalagen.

Övergångsregleringen bör innebära att de aktuella bestämmelserna inte behöver tillämpas förrän efter viss tid. Därigenom tydliggörs att polisen

får tillämpa bestämmelserna tidigare i den utsträckning de har möjlighet till det. Undantaget bör gälla generellt och inte, som föreslås i promemorian, enbart för uppgifter som har samlats in före ikraftträdandet. En övergångsperiod om drygt två år bör vara tillräcklig. Utgångspunkten bör vara att polisen vid utvecklingen av nya system och vid anpassningen av gamla skapar förutsättningar för att tillämpa bestämmelserna så snart som möjligt och att bestämmelserna tillämpas i den utsträckning det går.

Rikspolisstyrelsen framhåller att äldre information som samlats in i polisens underrättelseverksamhet inte alltid har åsatts en värdering av uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak och att det skulle kräva ett omfattande arbete att göra det i efterhand, om det ens är möjligt. Kravet på sådana upplysningar bör därför inte gälla för uppgifter som samlats in före ikraftträdandet.

De register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av den upphävda datalagen skiljer sig i flera avseenden åt sinsemellan. För vissa register är det dessutom svårt att överblicka vilka bestämmelser som gäller. Detta beror bl.a. på att Datainspektionen med stöd av datalagen har meddelat föreskrifter för registren och att dessa kan ha ändrats upprepade gånger. Med hänsyn till detta är det svårt att utforma detaljerade övergångsbestämmelser för behandlingen av personuppgifter i dessa register. Flera av dessa behöver dock anpassas till den nya lagen. I promemorian förslås en generell förlängning av övergångsbestämmelserna för nu aktuella register. Som *Datainspektionen* anför bör en generell förlängning undvikas.

För flertalet av de aktuella registren ger den föreslagna övergångsregleringen, med två år till ikraftträdande och undantag från tillämpningen av vissa bestämmelser, polisen tillräckligt utrymme att anpassa registren till den nya lagen. Vad gäller behandlingen av vissa kategorier av uppgifter kan det behövas bestämmelser i förordning som medger undantag från lagens bestämmelser om gallring och längsta tid för bevarande (se avsnitt 14.4). Detta gäller, som *Rikspolisstyrelsen* framhåller i sin redovisning, bl.a. uppgifter som för närvarande behandlas i datasystem och andra uppgiftssamlingar som rör uppgifter om gods samt efterlysta och försvunna personer.

För två register som förs med stöd av polisdatalagens övergångsbestämmelser behövs det dock särskilda övergångsbestämmelser. Det gäller signalements- och känneteckensregistret och det centrala brottsspaningsregistret.

I den nya lagen föreslås särskilda bestämmelser för fingeravtrycks- eller signalementsregister. De gallringsbestämmelser som föreslås är annorlunda än de som för närvarande gäller för signalements- och känneteckensregistret. Fram till den tidpunkt när Rikspolisstyrelsen har ändrat gallringsrutinen i registret bör detta få fortsätta att föras med stöd av samma regler som nu, dock längst till utgången av år 2014.

Om Rikspolisstyrelsen väljer att ha kvar det centrala brottsspaningsregistret krävs enligt styrelsen relativt omfattande anpassningar av detta till den nya regleringen. Detta motiverar särskilda övergångsbestämmelser för det registret. Registret bör på samma sätt som signalements- och känneteckensregistret få fortsätta att föras en tid med stöd av gällande regler, dock längst till utgången av år 2014.

Den personuppgiftsansvarige bör, liksom nu, kunna avanmäla ett register hos Datainspektionen. Genom en sådan avanmälan kommer polisen att kunna göra den nya lagen tillämplig på behandlingen redan innan den föreslagna övergångsperioden har löpt ut. Detta bör framgå av övergångsbestämmelserna.

19 En ny lag om polisens allmänna spaningsregister

19.1 Registret regleras i en tidsbegränsad lag

Regeringens förslag: Det nuvarande allmänna spaningsregistret ska under en övergångstid kunna bibehållas med stöd av en särskild författningsreglering. Registret ska regleras i en särskild lag. Den ska ge polisen möjlighet att registrera i huvudsak samma uppgifter som nu. Lagen ska ha begränsad giltighetstid. Registret ska föras av Rikspolisstyrelsen, som också ska vara personuppgiftsansvarig för detta.

Utredningens förslag: Det allmänna spaningsregistret bör författningsregleras. Registret särregleras i den nya polisdatalagen. Regleringen ska i allt väsentligt ge polisen rätt att fortsätta den behandling av personuppgifter som redan förekommer.

Remissinstanserna: Dåvarande *Riksskatteverket* och *Ekobrottsmyndigheten* har instämt i att det finns ett stort behov av det allmänna spaningsregistret. *Kustbevakningen* har ställt sig bakom en lagreglering. Övriga remissinstanser har inte yttrat sig.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta av remissinstanserna godtar eller kommenterar inte förslaget. *Tullverket* har förståelse för att man under en övergångsperiod behöver en särskild lag för registret men framhåller att regleringen så snart som möjligt bör arbetas in i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. *Datainspektionen* ifrågasätter behovet av en särskild lag och påpekar att så länge behandlingen i det nuvarande registret är förenlig med de allmänna bestämmelserna i den nya lagen behövs det ingen särreglering.

Skälen för regeringens förslag: Polisen för sedan år 1979 ett allmänt spaningsregister. Registret förs med stöd av den numera upphävda datalagen (1973:289) och Datainspektionens tillstånd samt övergångsbestämmelserna till polisdatalagen (1998:622). En närmare redogörelse för registret och dess innehåll finns i *bilaga 6*.

Polisdatautredningen, som hänvisar till starka krav från Rikspolisstyrelsen, framhåller att utredningens förslag till polisdatalag inte täcker alla de behov som det allmänna spaningsregistret avser att fylla. Misstankeregistret förutsätter att någon är skäligen misstänkt, men det finns behov av att kunna behandla uppgifter om personer mot vilka misstanken ligger på en lägre nivå. Kriminalunderrättelseregister kan inte heller fylla samma behov som det allmänna spaningsregistret, eftersom underrättelseregistren är inriktade på brottslig verksamhet, inte på konkreta brott. Utred-

ningen menar därför att det finns behov av ett allmänt spaningsregister och föreslår en särskild reglering av detta.

En grundläggande fråga är om det allmänna spaningsregistret behövs i polisens nya IT-miljö, eller om registret åtminstone på sikt kan ersättas med de möjligheter till behandling som öppnas genom den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Rikspolisstyrelsen har under arbetets gång hävdat att registret måste få finnas kvar, i vart fall tills vidare.

Det ursprungliga tillståndet att föra det allmänna spaningsregistret har ändrats genom ett flertal beslut, där framför allt registreringsgrunder har tillkommit och tagits bort. Det är därför svårt att överblicka vad tillståndet innebär. Tillståndet speglar också att det är fråga om ett register uppbyggt efter dåtidens teknik med begränsade sökmöjligheter. Oavsett behovet av registrering av vissa typer av uppgifter kan registret på sikt inte fortsätta att föras utan att det moderniseras och anpassas.

Regeringen anser att det allmänna spaningsregistret utgör ett viktigt arbetsredskap i polisens spaningsverksamhet. Den behandling av personuppgifter som förekommer i registret bör i allt väsentligt tillåtas även i fortsättningen. Den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ger en större frihet för polisen att registrera uppgifter än vad som föreslås av Polisdatautredningen. Det innebär att många av de uppgifter som nu registreras i det allmänna spaningsregistret på sikt kommer att kunna göras gemensamt tillgängliga i andra former. Det kommer emellertid att ta tid för polisen att bygga upp sin nya datastruktur. Under mellantiden finns det alltjämt ett behov av att behandla uppgifter i det allmänna spaningsregistret. Den behandling som den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet medger motsvarar inte i alla delar behandlingen i det nuvarande registret. Det är därför ingen lösning att, som *Datainspektionen* förespråkar, låta behandlingen i registret omfattas av de allmänna bestämmelserna i den lagen. Mot denna bakgrund delar regeringen promemorians uppfattning att registret tills vidare bör få finnas kvar som ett särskilt register.

Det allmänna spaningsregistret omfattar cirka 100 000 registrerade personer och innehåller känsliga uppgifter. Med hänsyn till registrets omfattning och innehåll finns det skäl att reglera registret i lag. Det är således inte lämpligt att genom övergångsbestämmelser låta registret fortsätta att föras på samma sätt som nu med stöd av tillstånd från Datainspektionen.

Registrets nuvarande utformning låter sig svårligen förenas med den systematik som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det sagda talar för att registret inte bör regleras i den lagen utan i en särskild lag. Ytterligare ett skäl för en sådan ordning är att den aktuella personuppgiftsbehandlingen på sikt bör anpassas till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och att, om det finns kvarstående behov som inte täcks av den lagen, det får övervägas om den bör ändras i något avseende. Den särskilda lagen om polisens allmänna spaningsregister bör därför, som föreslås i promemorian, ha begränsad giltighetstid. En tidsbegränsad lag ger polisen möjlighet att hinna bygga upp sin nya IT-struktur, samtidigt som den ger tydligt uttryck för att registret i dess

nuvarande form på sikt ska avvecklas. Den nya lagen bör utformas med utgångspunkt i att den ska reglera den behandling som för närvarande sker i det allmänna spaningsregistret.

Registret bör liksom nu föras av Rikspolisstyrelsen, som också bör vara personuppgiftsansvarig för registret.

19.2 Förhållandet till personuppgiftslagen

Regeringens förslag: Lagen ska gälla utöver personuppgiftslagen (1998:204).

Utredningens förslag innebär att nära nog alla regler i den föreslagna polisdatalagen ska gälla även för det allmänna spaningsregistret och att den lagen ska ersätta regleringen i personuppgiftslagen.

Remissinstanserna: De remissinstanser som har uttalat sig om det allmänna spaningsregistret har tillstyrkt att registret regleras i lag.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna har inga synpunkter på förslaget.

Skälen för regeringens förslag: I avsnitt 6.4 föreslås att personuppgiftslagen (1998:204) i väsentliga delar ska gälla vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet. I förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet har en lagstiftningsteknik valts som innebär att lagen innehåller dels en uttömmande uppräkning av de bestämmelser i personuppgiftslagen som ska tillämpas, dels ett antal bestämmelser som avviker från personuppgiftslagen. Syftet med detta är framför allt att underlätta för tillämparen. I bl.a. lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister används en annan lagstiftningsmodell. Den innebär att lagen enbart innehåller de särbestämmelser som ska gälla i förhållande till personuppgiftslagen, vilket får till följd att personuppgiftslagen blir tillämplig i övrigt. Enligt regeringens mening är detta en lämplig lösning när man särreglerar ett enskilt register. Den omständigheten att lagen föreslås ha en begränsad giltighetstid talar också för att regleringen bör vara så lagtekniskt enkel som möjligt. Samma lösning som används för misstankeregistret och belastningsregistret bör därför väljas i detta fall.

19.3 Registrets ändamål

Regeringens förslag: Det allmänna spaningsregistret ska ha till ändamål att utgöra underlag för systematisering av vissa personuppgifter som framkommit i polisens brottsbekämpande verksamhet. Registret får föras för att underlätta tillgången till sådan information som behövs i polisens spaningsverksamhet.

Personuppgifter i registret får behandlas för att tillhandahållas framför allt till myndigheter som bedriver brottsbekämpande verksamhet samt i viss utsträckning till annan verksamhet inom polisen.

Personuppgifter får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. I övrigt gäller 9 § första stycket d personuppgiftslagen (1998:204).

Utredningens förslag: Registret ska föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott.

Remissinstanserna: Endast *Rikspolisstyrelsen* har kommenterat registrets ändamål. Styrelsen har framhållit att polisen behöver kunna använda uppgifterna i registret även för den hjälpande verksamheten samt för handläggning av polismyndighetsärenden (t.ex. ärenden om vapenlicens). Styrelsen har föreslagit att spaningsregistret ska få användas för alla polisens uppgifter enligt 2 § polislagen (1984:387).

Promemorians förslag överensstämmer delvis med regeringens. I promemorian föreslås dock ingen reglering av sekundära ändamål och det primära ändamålet har utformats på ett delvis annat sätt.

Remissinstanserna: Endast *Rikspolisstyrelsen* och *Datainspektionen* kommenterar promemorians förslag i denna del. Rikspolisstyrelsen påpekar att det under den fortsatta beredningen bör klargöras att polismyndigheterna ska få tillgång till uppgifter ur registret för att fullgöra handräckningsuppdrag. Enligt Datainspektionen innebär förslaget en inskränkning i förhållande till det tillstånd som för närvarande reglerar innehållet i det allmänna spaningsregistret. Förslaget tar sikte på uppgifter som behövs för polisens spaning, medan tillståndet tar sikte på hantering av uppgifter från sådan spaning. Inspektionen framhåller vidare att lagstiftaren uttryckligen bör ange om registret ska vara ett spaningsregister för brottsutredningar eller om det också ska få användas i kriminalunderrättelseverksamhet.

Skälen för regeringens förslag: Bestämmelser om för vilka ändamål personuppgifter får behandlas har en central roll i registerförfattningar. Detta gäller såväl när författningen avser viss verksamhet som när den, som i detta fall, avser ett visst register.

Ändamålen för registret bör utformas efter samma principer som föreslås gälla för lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Först och främst bör de huvudsakliga ändamålen för registret anges (primära ändamål). Dessa ändamål bör kompletteras med ändamål som så uttömmande som möjligt anger i vilka fall uppgifter som behandlas i registret får tillhandahållas andra (sekundära

ändamål). Därutöver bör uppgifter få lämnas ut endast om utlämnandet är förenligt med den s.k. finalitetsprincipen (9 § första stycket d personuppgiftslagen).

En grundläggande fråga är för vilket eller vilka primära ändamål registret ska föras. Det nuvarande registret fyller den funktionen att det möjliggör registrering och spridning av uppgifter från polisens spaningsverksamhet. Denna verksamhet är inte författningsreglerad (utöver den spaning som utgör ett led i förundersökning; jfr 23 kap. 2 § rättegångsbalken). Spaningsverksamhet utgör inte heller längre en särskild aktivitetsgren inom polisen. Den ingår numera som en integrerad del både i verksamheten att förebygga, förhindra och upptäcka brott eller brottslig verksamhet och verksamheten att utreda och beivra brott.

Vid spaning är uppgifter om personer, både direkta och indirekta personuppgifter, intressanta. Spaningsverksamheten förutsätter framför allt behandling av personuppgifter som syftar till

– att finna gärningsmannen som har begått ett eller flera konkreta brott, om denne är okänd,

– att spåra en okänd person som visserligen är misstänkt därför att denne har setts på eller i närheten av en brottsplats men vars identitet inte är känd,

– att knyta en känd misstänkt person till viss brottslig verksamhet eller till ett konkret brott,

– att hitta samband mellan brott, eller

– att hitta en känd misstänkt person som håller sig undan polisen.

Spaning kan vidare användas för att finna kopplingar mellan personer som, utan att det finns någon konkret misstanke, kan antas kontinuerligt och aktivt engagera sig i brottslig verksamhet i någon form.

Spaning kan också ta sikte på misstänkta företeelser där man ännu inte har så robust underlag att anmälan om ett konkret brott kan upprättas. Som exempel kan nämnas att polisen bedriver spaning mot en lokal eller en bostad där man misstänker att det pågår exempelvis koppleri, narkotikaförsäljning eller olovlig försäljning av alkohol. Ofta grundar sig sådan spaning enbart på tips och iakttagelser om att det förekommer onormal trafik av personer till lokalen eller bostaden, vilket ger anledning att förmoda att någon form av olaglig verksamhet äger rum, även om man inte vet exakt vilken. Ett annat exempel där spaningen inte riktar sig mot konkreta brott är om det har förekommit upprepade brott inom ett visst geografiskt område, t.ex. bostadsinbrott, och polisen spanar i området i förhoppning om att påträffa den eller de skyldiga på bar gärning om de begår nya brott.

Datainspektionen påtalar att den ändamålsbeskrivning för registret som föreslås i promemorian är mer inskränkt än gällande ändamål för registret. Med hänsyn till det allmänna spaningsregistrets särdrag bör enligt regeringens mening ändamålen med registret utformas på annat sätt än för polisens personuppgiftsbehandling i den brottsbekämpande verksamheten i övrigt. Eftersom utgångspunkten är att i så stor utsträckning som möjligt ge stöd för nuvarande behandling, bör det primära ändamålet uttryckas på ett något annorlunda sätt än i promemorian och nära ansluta till ändamålet i gällande tillstånd. Registrets primära ändamål bör vara att utgöra underlag för systematisering av vissa personuppgifter som framkommit i polisens brottsbekämpande verksamhet. Registret bör få föras

för att underlätta tillgången till sådan information som behövs i polisens spaningsverksamhet. Uppgifter som behöver tas till vara för att finnas tillgängliga i sådan verksamhet bör således få registreras och struktureras i registret, för att tjäna som underlag för systematisering av uppgifter i spaningsverksamhet.

Datainspektionen anser vidare att lagstiftaren tydligt måste ange om registret ska vara ett spaningsregister för brottsutredningar eller om det också ska få användas i kriminalunderrättelseverksamhet. Av tillståndet för registret kan utläsas att detta är avsett att vara ett hjälpmedel vid såväl spaning som brottsutredning. Så bör vara fallet även när registret lagregleras. Enligt regeringens mening bör registret även kunna användas i underrättelseverksamheten i den meningen att uppgifter ur registret får tillföras den verksamheten. Däremot är det inte meningen att registreringen i det allmänna spaningsregistret ska ersätta den behandling av personuppgifter i underrättelseverksamhet som regleras i den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Det bör direkt av ändamålet med registret framgå att uppgifterna ska behövas i polisens spaningsverksamhet. Detta innebär att det ska finnas behov av att registrera uppgifter som en större krets av personer inom polisen bör kunna ha tillgång till för sitt spaningsarbete. Med den föreslagna utformningen av ändamålet faller uppgifter som enbart berör tidigare uppklarade brott i många fall utanför. Syftet är inte heller att registret ska innehålla uppgifter som skapar ett parallellt belastningsregister.

Kravet på att informationen behövs är således avsett att begränsa möjligheten att registrera uppgifter. Endast sådana uppgifter som har faktisk betydelse för polisens spaningsverksamhet i allmänhet, för brottsuppklaringen eller för spaningen i pågående brottsutredningar ska få registreras. Det ligger emellertid i sakens natur att det inte alltid går att på förhand avgöra om en viss uppgift har relevans för kommande spaningsverksamhet. Det bör därför räcka att det framstår som sannolikt att det finns ett behov av uppgiften i spaningsverksamheten. Avsikten är dock inte att registret ska kunna användas för att systematiskt kartlägga enskilda personer, vilkas brottslighet inte är så kvalificerad att personuppgifter om dem får behandlas med stöd av bestämmelserna om övervakning av brottsbelastade eller potentiellt farliga personer i den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

I promemorian föreslås inga sekundära ändamål för det allmänna spaningsregistret utan endast sekretessbrytande utlämnandebestämmelser. Som nämndes inledningsvis bör det emellertid – i likhet med vad som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet – finnas sekundära ändamål som så preciserat som möjligt anger i vilken utsträckning personuppgifter i registret får behandlas för att tillhandahållas brottsbekämpande verksamhet och annan verksamhet.

Uppgifter i registret bör naturligtvis kunna behandlas för att tillhandahålla information till Rikspolisstyrelsen och polismyndigheter i deras brottsbekämpande verksamhet. Vad som sägs i avsnitt 6.3 om Säkerhetspolisens tillgång till uppgifter bör på motsvarande sätt gälla för det allmänna spaningsregistret. Vidare bör uppgifter kunna tillhandahållas

Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket, om uppgifterna behövs i myndighetens brottsbekämpande verksamhet. Därutöver bör uppgifter under samma förutsättningar som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet kunna tillhandahållas utländska brottsbekämpande myndigheter eller organisationer.

På samma sätt som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör uppgifter vidare i viss utsträckning kunna lämnas till annan polisiär verksamhet än den brottsbekämpande. Av de skäl som anges i avsnitt 7.6 bör det, förutom vad gäller polisens handräckningsverksamhet, krävas särskilda skäl för att uppgifter ska få tillhandahållas sådan verksamhet.

Uppgifter bör också få behandlas för att tillhandahållas regeringen och riksdagen samt andra, om skyldighet att lämna uppgifter följer av lag eller förordning.

För att en uppgift ska få vidarebehandlas för något annat ändamål än de som nu angetts måste det i det enskilda fallet göras en bedömning att det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in. Detta följer av den s.k. finalitetsprincipen som kommer till uttryck i 9 § första stycket d personuppgiftslagen. I förtydligande syfte bör en hänvisning till denna bestämmelse tas in i lagen.

Det bör framhållas att ett utlämnande alltid måste vara förenligt med offentlighets- och sekretesslagen (2009:400), vilket ger ett grundläggande integritetsskydd. I syfte att underlätta uppgiftsutbytet mellan brottsbekämpande myndigheter föreslås i det följande sekretessbrytande bestämmelser.

19.4 Innehållet i registret

19.4.1 Vad ska kunna registreras?

Regeringens förslag: Lagen ska innehålla bestämmelser om vilka uppgifter som får behandlas i registret.

Uppgifter om en person ska som huvudregel få behandlas endast om

1. den som uppgiften avser kan misstänkas för ett brott, som inte har enbart böter i straffskalan, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

Även uppgifter om personer som inte kan misstänkas för brott ska dock få behandlas, om uppgiften har samband med en misstänkt person och behandlingen är av särskild betydelse för polisens spaningsverksamhet.

Därutöver får uppgifter om en juridisk person, ett transportmedel eller annat föremål som kan antas ha samband med ett brott behandlas, om behandlingen är av särskild betydelse för polisens spaningsverksamhet. Detta gäller dock inte om brottet har enbart böter i straffskalan.

Utredningens förslag: Uppgifter om en enskild person får registreras endast om den som avses med uppgiften kan misstänkas för att ha begått

ett brott och registreringen är av särskild betydelse för brottsbekämpningen. Uppgifter om transportmedel eller varor som kan antas ha samband med brott samt hjälpmedel som kan ha använts i samband med brott får registreras, även om uppgifterna kan hänföras till en person mot vilken det inte finns någon misstanke.

Remissinstanserna: Endast *Rikspolisstyrelsen* har yttrat sig om innehållet i registret. Synpunkterna avser det närmare innehållet i registret och redovisas därför i avsnitt 19.4.2.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Datainspektionen* vänder sig mot förslaget när det gäller förutsättningarna för registrering och anser att dessa innebär att det delvis blir en slump vilka uppgifter som får registreras. *Statens kriminaltekniska laboratorium* anser att det bör kunna registreras i det allmänna spaningsregistret att man vid sökning i DNA-register eller fingeravtrycksregister har funnit överensstämmelse mellan spår och uppgifter i de registren.

Skälen för regeringens förslag

Allmänna utgångspunkter

En utgångspunkt är att den nya regleringen av det allmänna spaningsregistret, så långt det kan motiveras av behov i den polisiära verksamheten, bör motsvara den registrering som sker nu. Samtidigt är det angeläget att man inte tillåter en registrering som inte är acceptabel med hänsyn till intresset av skydd för den personliga integriteten. Den enskilde bör i så stor utsträckning som möjligt ges samma skydd vid behandling av uppgifter i det allmänna spaningsregistret som vid behandling av uppgifter enligt den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Lagen bör därför inte bara innehålla regler om vad som krävs för att en person ska få registreras utan också om vilka andra uppgifter som får behandlas. Dessutom bör det införas begränsningar i fråga om vilka uppgifter som får vara sökbara i registret. Detta är begränsningar som i större eller mindre utsträckning har sin motsvarighet i det nuvarande tillståndet att föra det allmänna spaningsregistret.

Statens kriminaltekniska laboratoriums förslag om man ska kunna registrera ”träffar” i DNA-register eller fingeravtrycksregister saknar motsvarighet i dagens register. Eftersom utgångspunkten för den nya lagen är att skapa lagstöd för den typ av behandling som redan förekommer bör möjligheten till registrering inte utökas på det sätt som laboratoriet föreslår.

Datainspektionen menar att promemorians förslag leder till att förutsättningarna för att registrera uppgifter blir slumpmässiga eftersom det ställs som krav för registrering att det föreligger misstanke om ett konkret brott. Enligt tillståndet till det nuvarande registret ska registrering avse uppgifter med anknytning till misstänkt eller konstaterad brottslighet. Även enligt tillståndet krävs det således misstanke om planerade, förberedda, pågående eller fullbordade brott. Någon avgörande skillnad i förhållande till dagens registrering blir det således inte fråga om.

Uppgifter om misstänkta personer

För att en person ska få registreras bör det för det första krävas att han eller hon är misstänkt för ett brott. Det bör räcka med en låg grad av misstanke. Eftersom registret syftar till att underlätta spaningsarbetet, bör brott som i sin helhet har lagförts inte kunna läggas till grund för registreringen.

Rikspolisstyrelsens föreskrifter om det allmänna spaningsregistret (RPSFS 2003:4, FAP 448–1) innehåller en uppräkning av ett stort antal brottsbalksbrott (brott mot 3–4, 6, 8–14, 16 och 17 kap. brottsbalken) och vissa brott mot specialstraffrättsliga bestämmelser som utgör grund för registrering. En sådan uppräkning har bl.a. den nackdelen att den inte fångar in nya brottstyper. Som exempel kan nämnas att uppräkningen innehåller brott mot ransoneringslagen och valutabrott, som knappast förekommer, medan brott mot kreditupplysningslagen (1973:1173) inte täcks in, trots att det är en brottstyp som förknippas med brottslighet av organiserat slag.

Vid lagreglering av registret bör man enligt regeringens mening välja en mera generell lösning än en uppräkning av vissa brottstyper. En lämplig lösning är att avgränsa registreringen till personer som är misstänkta för brott som inte har enbart böter i straffskalan. Det kan nämligen inte anses motiverat att låta registret omfatta uppgifter om personer som är misstänkta enbart för bagatellbrott. Förslaget får till följd att å ena sidan några av de brottstyper som nu kan läggas till grund för registrering faller bort. Å andra sidan kan vissa nya brottstyper ligga till grund för registrering.

Förutom misstanke om brott av visst slag bör det krävas att behandlingen av personuppgifter är av särskild betydelse för polisens spaningsverksamhet. Kravet innebär att uppgifter som visserligen skulle ha allmänt värde för spaningsverksamheten, men där värdet inte är så stort, inte får behandlas. För att en uppgift ska anses ha särskild betydelse bör det krävas att den kan bidra till att brott, som är av sådan svårhetsgrad som krävs för behandling i registret, kan beivras. Det krävs en kvalificerad bedömning av om uppgifterna faktiskt har sådan betydelse. Endast ett fåtal tjänstemän får göra den bedömningen när det gäller den nuvarande registreringen. Detta bör gälla även i fortsättningen, men är inte något som behöver regleras i lagen.

Uppgifter om andra personer och om föremål

Det bör, på samma sätt som nu, vara möjligt att i registret behandla även uppgifter som avser personer som inte är misstänkta för brott. Sådana uppgifter bör dock få behandlas endast om uppgiften har anknytning till en misstänkt person. Vidare bör det krävas att behandlingen är av särskild betydelse för polisens spaningsverksamhet. För närvarande behandlas uppgifter om icke misstänkta i löpande text och är inte sökbara. Det rör sig t.ex. om uppgifter om att en viss namngiven person har setts i en misstänkt persons sällskap eller att den misstänkte brukar bo hos en namngiven anhörig. I det följande diskuteras vilka sökbegränsningar som bör gälla.

Polisen behöver vidare kunna behandla uppgifter om fordon och andra föremål som kan antas ha samband med ett brott. Det rör sig här om indirekta personuppgifter, t.ex. om registreringsnumret på ett fordon som uppges ha lämnat en brottsplats i hög fart i nära anslutning till brottet. I många fall tillhör sådana fordon helt oskyldiga personer, eftersom stulna bilar ofta används som flyktfordon. I andra fall kan uppgifter om fordonet leda till att gärningsmannen kan spåras. Uppgifter av detta slag bör kunna behandlas även i fortsättningen. En förutsättning för detta bör dock vara att uppgifterna är av särskild betydelse för polisens spaningsverksamhet.

Likaså har polisen behov av att i vissa fall, där det inte finns misstanke mot någon fysisk person, kunna registrera uppgifter om en juridisk person som kan antas ha samband med ett misstänkt brott. Det kan t.ex. röra sig om ett aktiebolag som äger eller disponerar en lokal där smuggelgods förvaras eller någon annan typ av juridisk person som äger eller hyr en lokal där alkohol eller narkotika tillverkas. Det kan även vara fråga om en juridisk person som har utfärdat vissa handlingar som utnyttjas i brottslig verksamhet. Samma förutsättningar som föreslås gälla för registrering av transportmedel bör gälla för registrering av juridiska personer.

19.4.2 Uppgifter om grunden för registreringen m.m.

Regeringens förslag: Registret ska alltid innehålla uppgifter om

1. grunden för att en person registreras som misstänkt eller att uppgifter om en juridisk person, ett transportmedel eller föremål införs i registret och omständigheterna i samband med detta,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än de som anges i 1 tillförs registret, och
3. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Någon upplysning om det sistnämnda behöver dock inte lämnas om det på grund av särskilda omständigheter är onödigt.

Därutöver får registret innehålla bl.a. följande uppgifter om en registrerad person:

– uppgift som är ägnad att identifiera personen,
– uppgift om vistelseadress,
– uppgift om verkställighet av påföljd för brott,
– uppgift om att personen är eftersökt i samband med brott,
– uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen, och
– uppgift om att personen är föremål för särskild övervakning.

Utredningens förslag motsvarar i stora delar promemorians. Utredningen förslår inte att grunden för registrering alltid ska antecknas.

Remissinstanserna: Rikspolisstyrelsen har tolkat förslaget så att man även i fortsättningen ska kunna markera i registret om en person tillhör landets allra grövsta brottslingar (s.k. A-markering) eller om vederbörande anses vara yrkeskriminell (s.k. Y-markering). Rikspolisstyrelsen anser att detta bör framgå direkt av lagtexten.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås inget undantag från kravet på att lämna upplys-

ningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak om detta på grund av särskilda omständigheter är onödigt.

Remissinstanserna: *Rikspolisstyrelsen* anser att ytterligare uppgifter om fordon och organisationer som har samband med brottslighet bör kunna registreras. Styrelsen framhåller också att det vid bekämpning av vardagsbrottsligheten finns ett stort behov av att kunna registrera uppgifter om vaneförbrytare (s.k. V-markerade). I övrigt berör remissinstanserna inte frågan.

Skälen för regeringens förslag: Lagen om polisens allmänna spaningsregister bör reglera både vilka uppgifter som alltid måste finnas i registret och vilka uppgifter som därutöver får behandlas.

Inledningsvis bör det framhållas att det allmänna spaningsregistret bygger på äldre teknik och att det därför inte medger fritextsökning utan endast sökning på vissa textfält eller begrepp. Eftersom lagen syftar till att reglera det nuvarande registret under en övergångsperiod, och därför också föreslås vara tidsbegränsad, bör innehållet i allt väsentligt spegla den nuvarande registreringen, även om detta kanske inte i alla delar överensstämmer med hur man numera brukar reglera register.

Vissa uppgifter i registret bör vara obligatoriska. För det första bör det alltid kunna utläsas vad som har motiverat att en person eller uppgifter om ett transportmedel eller annat föremål första gången har förts in i registret. Det måste således finnas uppgifter om det brott som har föranlett att en viss person har antecknats såsom misstänkt. Även omständigheterna kring brottet bör redovisas. Motsvarande krav bör ställas om det beträffande en registrerad person införs uppgifter om nya brottsmisstankar eller beträffande en juridisk person, ett transportmedel eller annat föremål införs nya uppgifter om samband med brott.

För det andra bör det framgå vad som har legat bakom att nya uppgifter av annat slag om en registrerad person tillförs registret. Här är det närmast fråga om vilka omständigheter eller händelser som gett upphov till den nya anteckningen. Det är nämligen vanligt att en registrering så småningom följs av nya noteringar om den registrerade personen, om uppgifterna är av värde från spaningssynpunkt. Det kan t.ex. röra sig om uppgifter om vilka personer en misstänkt narkotikabrottsling träffar, vilka fordon en misstänkt inbrottstjuv disponerar osv. Det är framför allt i sådana noteringar som det kan finnas uppgifter om personer som inte själva är misstänkta för brott.

Liksom nu bör också som huvudregel uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak bedömas. En sådan bedömning görs för närvarande av den person som avgör om uppgifterna har sådant värde från spaningssynpunkt att de över huvud taget bör tillföras registret. På samma sätt som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet (se avsnitt 10) bör någon upplysning inte krävas om det på grund av omständigheterna framstår som onödigt, t.ex. om det framgår att uppgifterna härrör från slutsatserna i en dom.

Av lagen bör också framgå vilka ytterligare uppgifter om den registrerade som får behandlas. Det bör vara fråga om uppgifter som typiskt sett är viktiga för polisens spaningsverksamhet och som i huvudsak motsvarar vad som nu får registreras i det allmänna spaningsregistret. Eftersom spaning kan äga rum av olika skäl bör det finnas utrymme för upp-

gifter som underlättar olika typer av spaning, framför allt uppgifter som underlättar personrelaterad spaning. Det rör sig exempelvis om uppgifter om var personen vistas, uppgifter som kan bidra till identifieringen av denne, uppgifter om anknytningen till juridiska personer och uppgifter som underlättar vid direkta ingripanden mot personen i fråga.

Rikspolisstyrelsen anser att vissa ytterligare uppgifter bör få registreras, bl.a. att en person är s.k. vaneförbrytare. En sådan registrering ter sig betänklig från integritetssynpunkt. Vidare kan behovet ifrågasättas mot bakgrund av att det framgår av belastningsregistret att en person har gjort sig skyldig till upprepade brott och av misstankeregistret om det finns flera aktuella misstankar. Någon registrering av vaneförbrytare på det sätt som Rikspolisstyrelsen förordar bör därför inte tillåtas.

För att så långt som möjligt anpassa regleringen till verksamhetens behov och för att uppnå ett tillfredsställande integritetsskydd, bör regeringen, eller den myndighet som regeringen bestämmer, meddela närmare föreskrifter om de uppgifter som får behandlas i registret och om förfarandet vid registreringen. En bestämmelse som informerar om att sådana föreskrifter kan meddelas bör införas i lagen.

19.5 Behandling av känsliga personuppgifter

Regeringens förslag: Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras, etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Uppgifter som behandlas på annan grund får dock kompletteras med sådana uppgifter, när det är absolut nödvändigt för syftet med behandlingen.

Uppgifter om en persons utseende ska alltid utformas på ett objektivt sätt med respekt för människovärdet.

Utredningens förslag överensstämmer i sak med promemorians, men utredningen föreslår inte någon särskild regel om uppgifter om personers utseende.

Remissinstanserna har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte i frågan.

Skälen för regeringens förslag: Det finns särskilda regler om behandling av känsliga personuppgifter både i 5 § polisdatalagen och i förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet (se avsnitt 8). En motsvarande bestämmelse bör införas i lagen om polisens allmänna spaningsregister.

Bestämmelsen bör utformas efter mönster av den bestämmelse som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det innebär att känsliga personuppgifter inte ska få behandlas enbart på grund av vad som är känt om personens ras, etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Däremot bör, om personuppgifter behandlas på annan grund, dessa få kompletteras med käns-

liga personuppgifter, men endast om detta är absolut nödvändigt för syftet med behandlingen. Vidare bör det införas en bestämmelse om att uppgifter om en persons utseende alltid ska utformas på ett objektivt sätt med respekt för människovärdet.

19.6 Särskilda upplysningar och sökbegränsningar

Regeringens förslag: När uppgifter behandlas som direkt kan hänföras till en person som inte misstänks för brott ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara i registret.

Vid sökning i registret får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp. Detta hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Tillgången till uppgifter i registret ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag överensstämmer i sak med promemorians vad gäller särskilda upplysningar. Utredningen föreslår inga sökbegränsningar.

Remissinstanserna har inte yttrat sig i saken.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna berör inte frågan.

Skälen för regeringens förslag: Som har framgått ovan bör det allmänna spaningsregistret få innehålla uppgifter om personer som inte är misstänkta för brott. Frågan är då i vilken utsträckning sådana uppgifter bör förses med särskilda upplysningar och vilka sökbegränsningar som bör gälla.

Lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet föreslås innehålla bestämmelser om att uppgifter som rör icke misstänkta personer, och som har gjorts gemensamt tillgängliga, som huvudregel ska förses med en upplysning om att personen i fråga inte är misstänkt (avsnitt 10). Motsvarande bör gälla för behandling av uppgifter i det allmänna spaningsregistret. Någon särskild upplysning bör dock inte krävas om det ändå av omständigheterna framgår att personen i fråga inte är misstänkt.

Uppgifter som direkt hänför sig till personer som inte själva är misstänkta bör inte få vara sökbara. Däremot bör indirekta personuppgifter som rör transportmedel och andra föremål kunna vara sökbara, på samma sätt som nu. Uppgifter av det slaget är viktiga från spaningssynpunkt, samtidigt som det integritetsintrång som en behandling kan medföra är begränsat. Uppgifter om fordon är tillgängliga i offentliga register och polisens behandling av dessa uppgifter kan inte sägas vara särskilt integritetskänslig. Detsamma gäller uppgifter om andra transportmedel. När det gäller andra föremål kan man inte dra lika generella slutsatser om ris-

ken för integritetsintrång, men eftersom uppgifterna kan ha stor betydelse för spaningsverksamheten, t.ex. en uppgift om varifrån ett visst skjutvapen härrör, bör en behandling som innebär att uppgiften är sökbar ändå kunna godtas.

Även uppgifter om juridiska personer bör, liksom nu, vara sökbara i registret. Sådana uppgifter har ofta ett stort spaningsvärde. I detta fall finns uppgifterna normalt också tillgängliga i offentliga register och det eventuella integritetsintrånget är därför begränsat.

Det bör införas samma begränsning vid sökning på känsliga personuppgifter som föreslås gälla i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Vid sökning i registret bör således uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte få användas som sökbegrepp. Detta bör inte hindra att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter, vilket bör framgå direkt av lagen. En motsvarande bestämmelse föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I avsnitt 6.6 redogörs för den närmare innebörden.

19.7 Utlämnande av uppgifter

Regeringens förslag: Personuppgifter som behövs för framställning av rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Om det är förenligt med svenska intressen, får personuppgifter lämnas till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott.

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

Trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400) har polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket rätt att ta del av personuppgifter i det allmänna spaningsregistret, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket ska kunna medges direktåtkomst till det allmänna spaningsregistret. En myndighet som får direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen har dock möjlighet att meddela föreskrifter om sådant utlämnande även i andra fall.

Utredningens förslag: Uppgifter ur det allmänna spaningsregistret ska få lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet, men endast om uppgifterna kan antas ha särskild betydelse för en pågående undersökning eller för andra brottsbekämpande åtgärder. Endast polismyndigheter ska kunna få direktåtkomst till registret.

Remissinstanserna: Flera remissinstanser, däribland *Sveriges domareförbund* och *Kammarrätten i Jönköping*, har ifrågasatt varför möjligheten att bevilja direktåtkomst generellt är så begränsad i utredningens förslag. Dåvarande *Riksskatteverket* har noterat att förslaget inte förefaller innebära någon förändring för skattebrottsenheternas del och framhållit behovet av samverkan mellan de brottsbekämpande myndigheterna.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian förslår dock inte att Skatteverket ska kunna medges direktåtkomst till registret.

Remissinstanserna: *Kustbevakningen* ställer sig bakom förslaget. *Rikspolisstyrelsen* anser att det bör övervägas att ge även Skatteverket möjlighet till direktåtkomst. *Skatteverket* anser att promemorians förslag bygger på en felaktig beskrivning av skattebrottsenheternas verksamhet och att verket bör medges direktåtkomst till registret.

Skälen för regeringens förslag

Sekretessbrytande bestämmelser

I avsnitt 12 diskuteras behovet av informationsutbyte för en effektivare brottsbekämpning. Vad som sägs där har giltighet även för det allmänna spaningsregistret. Detsamma gäller behovet av tillgång till uppgifter genom direktåtkomst. I avsnitt 13 övervägs behovet av sekretessbrytande bestämmelser. Uttalandena i det avsnittet har giltighet också för utlämnande av uppgifter ur det allmänna spaningsregistret. För att underlätta möjligheten att lämna ut uppgifter och bevilja direktåtkomst till registret bör det införas sekretessbrytande bestämmelser i den nya lagen. De bör utformas efter mönster av motsvarande bestämmelser i den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Det är framförallt polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket som i sin brottsbekämpande verksamhet kan ha behov av att få del av uppgifter ur registret (jfr avsnitt 19.3). Polismyndigheter och Ekobrottsmyndigheten (den polisiära verksamheten) har för närvarande direktåtkomst till registret, medan Tullverket, Kustbevakningen och Skatteverket i viss utsträckning kan få tillgång till uppgifter ur registret enligt 14 och 15 §§ polisdataförordningen (1999:81).

En regel om utlämnande av uppgifter bör först och främst tillgodose behovet av att kunna utbyta information inom polisväsendet. Vidare måste uppgifter kunna lämnas till andra brottsbekämpande myndigheter, eftersom brottsbekämpningen är en gemensam uppgift för flera myndigheter. De myndigheter som för närvarande har möjlighet att få uppgifter

ur det allmänna spaningsregistret bör kunna få det även när registret lagregleras. Mot den bakgrunden föreslås att polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket ska kunna få tillgång till uppgifter ur registret.

En grundläggande förutsättning för att uppgifter ska kunna lämnas ut bör vara att den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet. Här kan anmärkas att åtkomsten till uppgifter i det allmänna spaningsregistret, för myndigheter utanför polisväsendet, hittills har begränsats till sådana brottstyper som den mottagande myndigheten ska bekämpa. Som exempel kan nämnas Tullverket, vars åtkomst är begränsad till i huvudsak uppgifter om smuggling och om narkotikabrott. Begränsningar av det slaget behöver inte ställas upp i lag. Däremot bör lagen innehålla samma generella begränsning som den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, nämligen att tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Uppgifter som behövs för att framställa rättsstatistik bör alltid få lämnas ut till den statistikansvariga myndigheten. Motsvarande bestämmelser finns i andra lagar som reglerar behandlingen av personuppgifter i polisens brottsbekämpande verksamhet.

Slutligen bör lagen också innehålla en bestämmelse om utlämnande av uppgifter ur registret till utländska myndigheter och mellanfolkliga organisationer. Bestämmelsen bör utformas efter mönster av den bestämmelse som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Uppgifter ska således kunna lämnas till en utländsk polis- eller åklagarmyndighet (om staten är ansluten till Interpol), eller till Interpol eller Europol. Förutsättningarna för detta bör vara dels att utlämnandet är förenligt med svenska intressen, dels att uppgiften behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott. Vidare ska uppgifter kunna lämnas ut om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Den som överväger att lämna ut en uppgift till en mottagare utanför EU och EES-området måste dessutom alltid försäkra sig om att den mottagande staten eller organisationen har en adekvat nivå för skydd av personuppgifter, se 33 och 34 §§ personuppgiftslagen.

Den föreslagna regleringen motsvarar i huvudsak vad som gäller enligt polisdatalagen och polisdataförordningen.

Det finns inget skäl att införa en bestämmelse som reglerar utlämnande till utländsk underrättelse- eller säkerhetstjänst. Om frågan om utlämnande aktualiseras kan uppgifter lämnas ut efter en sedvanlig sekretessprövning.

I lagen bör det informeras dels om att regeringen har möjlighet att meddela föreskrifter om att uppgifter får lämnas ut även i andra fall, dels om att det även finns bestämmelser i offentlighets- och sekretesslagen om att uppgifter får lämnas ut, se t.ex. 8 kap 3 § nämnda lag.

Elektroniskt utlämnande av uppgifter

Liksom för övrig personuppgiftsbehandling inom polisen bör huvudregeln vara att endast enstaka uppgifter ur det allmänna spaningsregistret ska få lämnas ut på medium för automatiserad behandling (se avsnitt 12.4). Regeringen bör emellertid kunna meddela föreskrifter om undantag från denna begränsning på samma sätt som föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Fler myndigheter än vad Polisdatautredningen föreslog har numera möjlighet att få direktåtkomst till det allmänna spaningsregistret. De myndigheter som för närvarande har direktåtkomst bör kunna få det även när registret lagregleras. Det finns inget skäl att reglera direktåtkomsten till detta register på något annat sätt än direktåtkomsten till belastningsregistret eller misstankeregistret eller enligt den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. De uppgifter som får behandlas i dessa register och uppgiftssamlingar kan vara lika integritetskänsliga som uppgifter i det nu aktuella registret.

I promemorian föreslås rätten till direktåtkomst inte omfatta Skatteverket, under hänvisning till att Skatteverket inte bedriver spaningsverksamhet i fråga om brott med fängelse i straffskalan. Både *Rikspolisstyrelsen* och *Skatteverket* invänder mot förslaget i denna del. Eftersom Skatteverket i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet föreslås kunna få direktåtkomst till uppgifter av motsvarande slag, finns det inte skäl att utesluta möjligheten att ge myndigheten direktåtkomst till uppgifter i det nu aktuella registret. Skatteverket bör således finnas med i uppräkningen av myndigheter som har möjlighet att få direktåtkomst.

Det bör vara Rikspolisstyrelsen som bedömer dels om myndigheternas behov av uppgifter är så stort att direktåtkomst är motiverad, dels om det är möjligt att bevilja direktåtkomst med hänsyn till mottagarens datasäkerhet m.m. Rikspolisstyrelsen kan givetvis, på samma sätt som nu, begränsa åtkomsten till vissa typer av uppgifter eller till uppgift om huruvida någon förekommer i registret eller inte.

I lagen bör informeras om att regeringen, eller den myndighet regeringen bestämmer, har möjlighet att meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

19.8 Gallring

Regeringens förslag: Uppgifter om en misstänkt person ska gallras senast tre år efter det att en uppgift om att han eller hon kan misstänkas för ett brott registrerades. Avser uppgiften misstanke om ett brott med lägst två års fängelse i straffskalan, behöver uppgifterna dock inte gallras förrän efter fem år.

Om en ny uppgift om den misstänkte införs före utgången av den tid som anges i första stycket kan gallringstiden förlängas. Uppgifter om en person som inte är misstänkt för brott ska gallras senast samtidigt som uppgifterna om den misstänkta personen gallras.

Uppgifter om en juridisk person, ett transportmedel eller annat föremål, som har registrerats utan anknytning till någon misstänkt person, ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott med lägst två års fängelse i straffskalan, behöver uppgifterna dock inte gallras förrän fem år efter att den senaste uppgiften infördes.

Regeringen har möjlighet att meddela föreskrifter om att uppgifter, trots bestämmelser om gallring, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Om det finns synnerliga skäl får regeringen eller den myndighet som regeringen bestämmer i ett enskilt fall besluta om att en uppgift får bevaras under längre tid än vad som är tillåtet enligt lagens gallringsbestämmelser.

Utredningens förslag: Personuppgifter ska gallras ur det allmänna spaningsregistret senast tre år efter det att uppgifter om att den registrerade kan misstänkas ha begått brott senast infördes. Om den senaste händelsen avser misstanke om ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, ska dock uppgifterna få stå kvar i fem år efter den senaste registreringen.

Remissinstanserna: *Rikspolisstyrelsen,* dåvarande *Riksåklagaren* och dåvarande *Kriminalvårdsstyrelsen* har alla kritiserat utredningens förslag om gallringsfrister och hävdat att vissa uppgifter bör få behandlas längre.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser att förslaget har samma brister som förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Förslaget kan enligt inspektionen inte anses uppfylla kraven på en behovsprövning i enlighet med dataskyddskonventionen, bl.a. med hänsyn till att gallringsreglerna inte tar hänsyn till resultatet av straffprocessen eller att brottsmisstanke inte längre finns.

Skälen för regeringens förslag: Gallringsreglerna för det allmänna spaningsregistret är komplicerade. Fristerna knyter an dels till brottets svårhetsgrad med tre olika frister (fem år, tre år och 18 månader), dels till typen av uppgift som registrerats (t.ex. 6 månaders gallringsfrist för transportmedel), dels till förekomsten av nya uppgifter om den registrerade. I det sistnämnda fallet innebär gallringsreglerna att vissa typer av noteringar medför en något längre och andra en något kortare gallringstid. Något förenklat kan man säga att uppgifter av mer begränsat spaningsvärde (t.ex. uppgifter om fordon) gallras tidigare än uppgifter som

generellt sett anses ha större spaningsvärde (t.ex. uppgifter om samröre med andra personer). Om det införs nya uppgifter i registret om den registrerade personen eller objektet, förlängs gallringsfristen, i vissa fall 18 månader och i andra fall kortare tid. Uppgifter om en person gallras omedelbart i vissa fall där det står klart att det inte längre finns någon brottsmisstanke. Slutligen finns det även en bestämmelse som hindrar gallring i vissa fall.

Remisskritiken avseende Polisdatautredningens förslag visar att en enhetlig gallringsregel av det slag som utredningen föreslår inte i tillräcklig utsträckning tillgodoser verksamhetens behov. Det är å andra sidan inte lämpligt att i en lag skapa så svåröverskådliga gallringsregler som tillämpas för det allmänna spaningsregistret för närvarande. Behovet av en effektiv verksamhet talar för att uppgifter som är viktiga för spaningsverksamheten ska kunna bevaras. Mot det står att uppgifterna i det allmänna spaningsregistret dels rör ett stort antal personer, dels kan avse misstankar som inte är så fast underbyggda att de kan registreras i misstankeregistret. Att bevara sådana uppgifter under en längre tid innebär risk för integritetsintrång. *Datainspektionen* invänder bl.a. mot att gallringsreglerna inte tar tillräcklig hänsyn till ändrade förhållanden.

Inledningsvis bör det erinras om att registret i fråga förs sedan 1970-talet med Datainspektionens tillstånd. Inspektionen har, såvitt känt, inte meddelat några gallringsregler för registret. Därför gäller endast de allmänna gallringsbestämmelserna i den upphävda datalagen (1973:289).

Rikspolisstyrelsen gallrar uppgifter ur registret enligt vissa principer. En utgångspunkt är att uppgifter som inte är rena identitetsuppgifter och uppgifter om hur personen kan nås (adress, telefonnummer m.m.), uppgifter om brott eller uppgifter om verkställighet av påföljd eller vård i stor utsträckning antecknas i s.k. notiser. Gallring sker bl.a. när det inte finns några aktuella notiser om personen, när uppgifterna inte längre behövs och när den misstänkte blir 80 år. När det gäller uppgifter om brott sker gallring bl.a. om brottsmisstanken avskrivs på grund av att vederbörande ansetts oskyldig eller gärningen inte utgör brott.

Enligt regeringens mening är det inte rimligt att vid lagreglering av registret ställa krav på helt nya gallringsregler, eftersom det kan kräva kostsamma ombyggnader av det tekniskt ålderdomliga registret. Gallringsreglerna bör således, som föreslås i promemorian, utformas i huvudsak med utgångspunkt i hur gallringen görs för närvarande.

En rimlig avvägning mellan intresset av att bekämpa brott och integritetsskyddsintresset är, som Polisdatautredningen och promemorian föreslår och som i stor utsträckning redan tillämpas, gallringsfrister på tre respektive fem år, beroende på vilket brott misstanken avser. Om det tillkommer nya brottsmisstankar, bör enligt regeringens mening gallringsfristen på motsvarande sätt kunna förlängas med tre respektive fem år. Om registret tillförs andra uppgifter som är av särskilt värde för spaningsverksamheten, bör tiden för gallring också flyttas fram, men då bara med ett år.

På motsvarande sätt bör gallringsfristen för uppgifter om en juridisk person, ett transportmedel eller annat föremål som har införts i registret utan samband med en registrerad person konstrueras med utgångspunkt i det misstänkta brottet. Uppgifterna bör således gallras senast efter tre

respektive fem år, med möjlighet till förlängning av gallringsfristen om en ny uppgift som kan antas ha samband med ett brott antecknas.

I de fall där registret har tillförts uppgifter om en person som inte själv kan misstänkas för brott men som har samband med en registrerad person, bör uppgifterna gallras senast samtidigt som uppgifterna om den registrerade personen gallras.

De föreslagna gallringsreglerna anger när uppgifterna senast ska gallras. Om det kommer fram omständigheter som gör att en registrerad uppgift inte längre behövs ska uppgiften gallras tidigare. Av de grundläggande bestämmelserna i personuppgiftslagen följer att personuppgifter inte får bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Gallringsfristerna utgör en ram. Närmare föreskrifter bör meddelas av regeringen eller av den myndighet som regeringen bestämmer. I lagen bör det införas en bestämmelse som informerar om att sådana föreskrifter kan meddelas. Det kan finnas skäl att överväga kortare gallringsfrister för vissa typer av uppgifter, t.ex. för uppgifter om fordon.

Regeringen eller den myndighet som regeringen bestämmer bör ha möjlighet att, trots gallringsbestämmelser, meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål.

Om det finns synnerliga skäl, bör regeringen, eller den myndighet som regeringen bestämmer, även i ett enskilt fall kunna besluta att en uppgift får bevaras under längre tid. Det skulle t.ex. kunna gälla en person som övervakas enligt 3 kap. 2 § första stycket 2 lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och som polisen vet befinner sig utomlands. Sådana beslut bör omprövas årligen. Ett beslut om att uppgifter ska bevaras trots att den normala gallringsfristen har löpt ut bör därför dokumenteras.

De närmare detaljerna kring gallringen utvecklas i författningskommentaren.

19.9 Övriga frågor

19.9.1 Rättelse och skadestånd m.m.

Regeringens förslag: Bestämmelserna i personuppgiftslagen om rättelse och skadestånd ska gälla för behandling enligt lagen.

Utredningens förslag motsvarar i sak promemorians.

Remissinstanserna har tillstyrkt förslaget eller inte haft några synpunkter på det.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna framför inte några synpunkter.

Skälen för regeringens förslag: På motsvarande sätt som inom andra områden kan det inte uteslutas att personuppgifter som behandlas med stöd av de nya bestämmelserna vid en kontroll i efterhand visar sig vara behäftade med felaktigheter. För sådana fall bör den registrerade vara berättigad till rättelse och skadestånd under samma förutsättningar som gäller för behandling som omfattas av personuppgiftslagen, dvs. enligt 28

och 48 §§ personuppgiftslagen. Med hänsyn till hur dessa regler är utformade måste en särskild hänvisning göras till dem för att de ska gälla för behandling som sker enligt den nya lagen (jfr prop. 1997/98:97 s. 90).

Tillsyn över polisens personuppgiftsbehandling enligt denna lag bör enligt regeringens mening utövas enligt samma regler som föreslås gälla i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet (avsnitt 17.2).

19.9.2 Ikraftträdande m.m.

Regeringens förslag: Lagen ska träda i kraft den 1 mars 2012 och gälla till utgången av februari 2017. I fråga om uppgifter som har samlats in före ikraftträdandet behöver någon upplysning inte lämnas om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Utredningen har inget motsvarande förslag.

Remissinstanserna har inte berört frågan.

Promemorian föreslår att lagen ska träda i kraft samtidigt som lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och gälla i fem år därefter.

Remissinstanserna tar inte upp inte frågan.

Skälen för regeringens förslag: Som redan påpekats är lagregleringen av det allmänna spaningsregistret en åtgärd som är avsedd att under en övergångsperiod lösa polisens behov av att kunna registrera vissa uppgifter som behövs i spaningsverksamheten. Regeringen delar promemorians uppfattning att lagen bör vara tidsbegränsad och att en period om fem år räknat från ikraftträdandet av den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör vara tillräcklig för att polisen ska kunna fasa ut registret i dess nuvarande form. I likhet med vad som föreslås i övergångsbestämmelserna till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör kravet på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak inte gälla för uppgifter som samlats in före ikraftträdandet.

I avsnitt 17.3 har behovet av utvärdering av den nya lagstiftningen behandlats. I utvärderingen bör det ingå att ta ställning till om regleringen fullt ut tillgodoser polisens verksamhetsbehov bl.a. när det gäller uppgifter som registreras i det allmänna spaningsregistret. Eftersom lagen om polisens allmänna spaningsregister föreslås vara tidsbegränsad finns det anledning att överväga den frågan i god tid före den tidpunkt när lagen enligt förslaget upphör att gälla.

20 Följdändringar m.m.

Regeringens förslag: Hänvisningar i andra lagar till polisdatalagen eller till register som förs med stöd av den lagen ändras till hänvisningar till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller, i vissa fall, till lagen om polisens allmänna spaningsregister. Bestämmelserna i säkerhetsskyddslagen om registerkontroll anpassas till den nya regleringen. Korrigeringar görs i två bestämmelser i offentlighets- och sekretesslagen.

Utredningens förslag överensstämmer i huvudsak med promemorians.

Remissinstanserna har inte yttrat sig i saken.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås dock en bestämmelse om vilken kontroll som alltid ska utföras vid registerkontroll samt en informationsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av registerkontrollen.

Remissinstanserna: Med undantag av *Säkerhetspolisen* kommenterar remissinstanserna inte promemorians förslag. Säkerhetspolisen anser att förslaget om ändring i säkerhetsskyddslagen innebär en saklig förändring som inte tillgodoser myndighetens behov.

Skälen för regeringens förslag

Följdändringar

I ett antal lagar finns det hänvisningar till polisdatalagen (1998:622) eller till vissa register som förs med stöd av den lagen. Dessa hänvisningar bör ersättas med hänvisningar till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och, i vissa fall, lagen om polisens allmänna spaningsregister. Ändringar av detta slag bör göras i rättegångsbalken, lagen (2000:344) om Schengens informationssystem, lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och offentlighets- och sekretesslagen (2009:400). Med undantag av förslaget till ändring i 18 kap. 2 § offentlighets- och sekretesslagen innebär förslagen inga förändringar i sak. Ändringen i den sistnämnda bestämmelsen är en nödvändig konsekvens av att underrättelseverksamhet inte regleras på samma sätt i den nya lagen som i polisdatalagen. Tillämpningsområdet är dock i allt väsentligt detsamma som i den nuvarande regleringen. Motsvarande ändring gjordes när den nu gällande lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet beslutades.

Det krävs även ändringar i säkerhetsskyddslagen (1996:627). I 12 § säkerhetsskyddslagen behandlas sådan registerkontroll som görs inom ramen för en säkerhetsprövning. Enligt paragrafen avses med registerkontroll dels att uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller polisdatalagen, dels att uppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen annars behandlar. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild utredning. Bestämmelsen fick sin nuvarande lydelse efter förslag i pro-

positionen Polisens register som resulterade i polisdatalagen (prop. 1997/98:97). Dessförinnan avsågs med registerkontroll ”att uppgifter hämtas från polisregister”. I författningskommentaren i propositionen angavs att ändringen var en följd av att polisregisterbegreppet inte längre används i den betydelse det tidigare haft men att någon ändring i sak i förhållande till gällande rätt inte var avsedd.

Registerkontrollen utgör en del av den säkerhetsprövning som syftar till att pröva en persons pålitlighet från säkerhetssynpunkt, för att förebygga att personer som inte är pålitliga deltar i verksamhet som har betydelse för rikets säkerhet. Registerkontrollens omfattning är olika beroende på om personen i fråga är placerad i säkerhetsklass 1, 2 eller 3.

I promemorian föreslås vissa ändringar i sak när det gäller 12 § säkerhetsskyddslagen, bl.a. föreslås en reglering av vilken kontroll som alltid ska utföras vid en registerkontroll. *Säkerhetspolisen* kritiserar förslaget och anför bl.a. att omfattningen av registerkontrollen indirekt framgår av andra bestämmelser i säkerhetsskyddslagen och att det inte finns något behov av att reglera vilken kontroll som alltid ska utföras.

Regeringen har initierat ett arbete med en allmän översyn av säkerhetsskyddslagen. Säkerhetspolisen har fått i uppdrag att utföra en förstudie över de frågeställningar som myndigheten anser bör behandlas i översynen (Ju2009/5174/PO). Mot bakgrund härav, och med beaktande av *Säkerhetspolisens* synpunkter, bör utgångspunkten vara att i nuläget göra så lite förändringar som möjligt i den nuvarande regleringen. Vissa ändringar krävs dock. Lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ska vara teknikneutral och i princip inte reglera enskilda register eller hur polisen ska strukturera sin information. Personuppgifter som kan vara av betydelse för registerkontrollen kommer därför inte enbart att behandlas i traditionella register. Därtill kommer att begreppet särskild undersökning inte används i den nya lagen. Bestämmelserna om registerkontroll i säkerhetsskyddslagen måste därför i viss utsträckning anpassas till den nya lagstiftningen.

Det är enligt regeringens mening rimligt att en registerkontroll omfattar uppgiftsinhämtning från polisens allmänna spaningsregister. Den lagen bör därför finnas med i uppräkningen i 12 § säkerhetsskyddslagen. Vidare bör bestämmelsen ge utrymme för inhämtande av uppgifter som behandlas enligt lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, vilket motsvarar hänvisningen till polisdatalagen. Frågan är då om det bör införas någon motsvarighet till den begränsning i gällande rätt som består i att registerkontroll inte omfattar att uppgifter hämtas från en förundersökning eller en särskild undersökning. Någon motsvarighet till särskild undersökning kommer inte att finnas i den nya lagstiftningen, varför någon sådan begränsning inte är möjlig. Enligt regeringens mening bör regleringen inte heller utesluta att Säkerhetspolisen har möjlighet att ta del av uppgifter från förundersökningar.

Avsikten är emellertid inte att ändringarna ska innebära några praktiska förändringar i förhållande till den registerkontroll som utförs av Säkerhetspolisen enligt nuvarande reglering.

Ändringar i offentlighets- och sekretesslagen

Den sekretessbrytande regeln i 18 kap. 18 § offentlighets- och sekretesslagen (som motsvarar 5 kap. 7 § andra stycket andra meningen sekretesslagen) omfattar, på grund av ett förbiseende i lagstiftningsarbetet, all sekretess enligt 17 §. Avsikten var att sekretessgenombrottet liksom tidigare enbart skulle omfatta andra stycket i 17 §, dvs. uppgifter som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Eftersom det är fråga om ett uppenbart misstag bör regeln ändras så att den motsvarar vad som tidigare gällde, dvs. sekretessgenombrottet bör enbart omfatta andra stycket. Ändringen bör tas upp som ett särskilt lagförslag, eftersom den bör träda i kraft tidigare än de övriga lagförslagen.

På grund av att vissa av kapitlen i offentlighets- och sekretesslagen numrerades om i propositionen i förhållande till lagrådsremissen uppkom en felaktig hänvisning i den nuvarande lydelsen av 35 kap. 1 §. Hänvisningen i paragrafens första stycke, punkten 9, till 4 kap. 1 § samma lag är uppenbart felaktig. Den bör ersättas med en hänvisning till 5 kap. 1 §. Även denna ändring bör träda i kraft tidigare än lagförslagen i övrigt.

Övergångsbestämmelser

Det krävs övergångsbestämmelser till de ändringar i offentlighets- och sekretesslagen som föreslås träda i kraft samtidigt som lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För övriga i detta avsnitt föreslagna ändringar krävs inte några övergångsbestämmelser.

21 Konsekvenserna av förslagen

Regeringens bedömning: Förslagen innebär att polisen behöver genomföra anpassningar av befintliga datasystem. Kostnaderna för detta bör finansieras inom ramen för polisens anslag. Kostnaderna för Säkerhets- och integritetsskyddsnämndens utökade tillsyn bör finansieras inom ram på statsbudgeten.

Utredningen utgår från att kostnaderna finansieras inom polisens anslag.

Remissinstanserna har inte haft några synpunkter.

Promemorians bedömning: Förslagen ger inte upphov till kostnader som inte kan täckas av myndigheternas befintliga anslag.

Remissinstanserna: *Rikspolisstyrelsen* anger i sitt remissvar att om den nya lagstiftningen skulle kräva anpassning av samtliga centrala och lokala datasystem inom polisen skulle den totala kostnaden kunna uppgå till cirka 500 miljoner kronor, men att beräkningen dels är mycket osäker, dels utgår från att lagen ska träda i kraft redan efter två år. Med en femårig övergångsperiod skulle det inte krävas en så omfattande anpassning av befintliga system. *Säkerhets- och integritetsskyddsnämnden* förutsätter att nämnden tillförs nya resurser för den utökade tillsynen och beräknar kostnaden för detta till 4,5 miljoner kronor per år. *Datainspek-*

tionen framhåller att, eftersom lagförslaget är komplext och svårtolkat samt att det förutsätter visst samråd mellan polisen och inspektionen, inspektionens resurser måste förstärkas för att den ska kunna utöva avsedd tillsyn över polisens personuppgiftsbehandling. Fackförbundet *TULL-KUST* ifrågasätter allmänt promemorians bedömning angående de ekonomiska konsekvenserna.

Skälen för regeringens bedömning

Ekonomiska konsekvenser

Förslagen ger de rättsliga förutsättningarna för att polisen ska kunna bygga upp ett nytt verksamhetsstöd för en modern informationshantering och i samband med detta kunna avveckla äldre register. Den nationella mobiliseringen mot brott och kampen mot den organiserade brottsligheten förutsätter att den information som polisen förfogar över är lättillgänglig och att den på ett enkelt och effektivt sätt kan spridas till andra myndigheter som har behov av den. Vidare utgör informationshanteringen hos polisen nyckeln till en effektivare informationshantering inom hela rättskedjan. Att polisens informationshantering är effektiv är således ett övergripande intresse för statsförvaltningen.

Jämfört med den nuvarande regleringen innebär förslagen att polisen ges bättre förutsättningar att använda modern teknik i den brottsbekämpande verksamheten. Detta, i förening med förbättrade och förenklade möjligheter att lämna ut uppgifter både till andra brottsbekämpande myndigheter och till andra myndigheter i syfte att samverka mot brott, bör kunna leda till såväl en ökad brottsuppklarning som vissa ekonomiska besparingar. De ekonomiska besparingarna kommer emellertid först på sikt när äldre system har kunnat ersättas.

Vid redovisningen av det uppdrag till Rikspolisstyrelsen som beskrivs i avsnitt 3 har styrelsen försökt uppskatta kostnaderna för anpassningen av nuvarande system till en ny lagstiftning, men framhåller att de exakta kostnaderna inte kan anges utan närmare förstudier. Styrelsen påpekar även att man bör undvika kostnader för anpassning av system som man vet ska fasas ut och ersättas med nya system. Styrelsen förordar därför en generell övergångstid om tre år samt undantag från vissa av den nya lagens bestämmelser under ytterligare två år. Med detta som utgångspunkt uppskattar styrelsen kostnaderna för bl.a. ändrad teknik, inklusive förstudier, till sammanlagt cirka 200 miljoner kronor, fördelat över tiden fram till dess att lagen har trätt i kraft i sin helhet. Kostnaden för anpassning av nuvarande fingeravtrycksregister är dock inte medräknad.

Den framtida utvecklingen av teknik och system för personuppgiftsbehandling läggs i stor utsträckning i händerna på polisen, genom att lagstiftningen inte längre i samma utsträckning som hittills bygger på en reglering av vilka register som får föras. Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet reglerar ramarna för behandlingen. Samtidigt innehåller annan lagstiftning krav på polisens arbete som i många avseenden styr vilken personuppgiftsbehandling som behövs. Utvecklingen när det gäller elektroniskt informationsflöde i rättskedjan spelar också roll. Regeringen bedömer att den nya

regleringen kommer att medföra vissa begränsade kostnader för ändringar i de nuvarande systemen.

I avsnitt 19, som behandlar ikraftträdande- och övergångsbestämmelser, föreslås att lagen ska träda i kraft den 1 mars 2012 och att några av lagens bestämmelser inte behöver tillämpas förrän år 2015. Vidare föreslås särskilda övergångsbestämmelser för ett fåtal register. Härigenom tillgodoses *Rikspolisstyrelsens* krav på en längre tid för anpassning av datasystemen än den som föreslogs i promemorian, i syfte att minska kostnaderna. Vid planering och anskaffning av nya system ska den nya lagstiftningen beaktas. Några särskilda kostnader utöver vad som uppstår inom ramen för ordinarie utvecklingsarbete förutses inte. De kostnader som uppstår för polisen ska finansieras inom ramen för polisens anslag.

Det vidgade tillsynsansvar som föreslås för Säkerhets- och integritetsskyddsnämnden kommer att medföra ökade kostnader för nämnden. Dessa kostnader ska finansieras inom ram på statsbudgeten.

För Datainspektionens del innebär lagförslagen inte några nya uppgifter. Det förhållandet att en ny lagstiftning är mera komplex än den nuvarande motiverar inte att myndigheten tillförs ytterligare resurser. Den begränsade samrådsskyldighet som diskuteras i avsnitt 17.2 bör kunna hanteras inom myndighetens ordinarie anslag.

Några merkostnader för andra brottsbekämpande myndigheter förutses inte. Eventuella merkostnader ska dock finansieras inom befintliga ramar.

Andra konsekvenser

Förslagen kommer att möjliggöra en effektivisering av polisens arbete med inhämtning, bearbetning och analys av information både i underrättelseverksamheten och vid utredning och beivrande av brott. Vidare skapas bättre förutsättningar för att kunna nyttiggöra all den information som polisen förfogar över. Dessutom utökas möjligheterna att utbyta information mellan polisen och andra brottsbekämpande myndigheter, vilket också effektiviserar brottsbekämpningen. Förutsättningarna för polisen att tillsammans med andra myndigheter effektivt samverka mot brott förbättras också. Sammantaget kommer således reformen att ha en positiv effekt på det brottsförebyggande arbetet och att skapa bättre förutsättningar för polisen och övriga brottsbekämpande myndigheter att effektivt bekämpa brottsligheten.

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

22 Författningskommentar

22.1 Förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

1 kap. Lagens syfte och tillämpningsområde

Lagens syfte

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter i polisens brottsbekämpande verksamhet samt att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sådan verksamhet.

I paragrafen anges det övergripande syftet med lagen. Detta överensstämmer delvis med syftet med personuppgiftslagen (1998:204), dvs. att skydda människor mot att deras personliga integritet kränks. Därutöver syftar lagen till att tillgodose intresset av att polisen ska kunna bedriva en effektiv brottsbekämpning. Motiven till bestämmelsen har redovisats i avsnitt 6.2.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Lagen gäller inte vid behandling av personuppgifter enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2010:000) om polisens allmänna spaningsregister.

Lagen gäller inte heller när personuppgifter behandlas i vapenregister med stöd av vapenlagen (1996:67), om inte detta särskilt anges i den lagen.

Paragrafen anger lagens tillämpningsområde. Frågan har behandlats i avsnitt 6.3.

I *första stycket* anges inledningsvis att lagen gäller vid ”behandling av personuppgifter”. Med personuppgifter avses detsamma som i 3 § personuppgiftslagen (1998:204), dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Också begreppet behandling har samma innebörd som i den paragrafen. Därmed avses således varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, t.ex. insamling, registrering, organisering, lagring, bearbetning, användning, spridning eller annat tillhandahållande, sammanställning eller samkörning samt utplåning eller förstöring.

För att denna lag 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 (jfr 5 § personuppgiftslagen som innehåller samma rekvisit). Utanför lagens till-

lämpningsområde faller således helt manuell behandling av personuppgifter som inte ingår i någon samling som är tillgänglig för sökning.

Av första stycket följer vidare att lagen endast är tillämplig i polisens brottsbekämpande verksamhet. Med brottsbekämpande verksamhet avses i detta sammanhang den verksamhet för vilken personuppgifter får behandlas enligt 2 kap. 7 § eller 5 kap. 1 §. I avsnitt 7.2–7.4 och 16.3.2 samt i kommentaren till nyss nämnda paragrafer lämnas en närmare redogörelse för den verksamhet som här avses med begreppet brottsbekämpande verksamhet. Lagen är däremot inte tillämplig på annan verksamhet som polisen bedriver, t.ex. hjälpande verksamhet eller verksamhet för att upprätthålla ordning och säkerhet utan anknytning till brottsbekämpning. För behandling av personuppgifter i sådan verksamhet gäller i stället bestämmelserna i personuppgiftslagen. Därmed faller också en del av polisens register utanför den nya lagens tillämpningsområde, t.ex. polisens adressdatabas, polisens fastighetsfråga och polisens folkbokföringsdatabas samt passregistret. I vilken utsträckning uppgifter från dessa register får användas i den brottsbekämpande verksamheten får alltså bedömas enligt personuppgiftslagen. Däremot är det bestämmelserna i denna lag som avgör i vilken utsträckning personuppgifter som har samlats in i den brottsbekämpande verksamheten får tillhandahållas polisens övriga verksamhet (främst 2 kap. 8 § första stycket 3 och 4).

Polisen bedriver brottsbekämpande verksamhet vid Rikspolisstyrelsen och polismyndigheterna samt vid Ekobrottsmyndigheten. I första stycket klargörs att lagen gäller oavsett vid vilken av dessa myndigheter som personuppgiftsbehandlingen sker. Personuppgiftsbehandling vid Ekobrottsmyndigheten som inte hänför sig till polisens brottsbekämpande verksamhet faller således utanför lagens tillämpningsområde.

I *andra stycket* föreskrivs att lagen inte gäller vid sådan personuppgiftsbehandling som sker med stöd av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen om polisens allmänna spaningsregister. Detta överensstämmer, förutom såvitt avser personuppgiftsbehandling som sker med stöd av den sistnämnda lagen, med vad som gäller enligt 1 § tredje stycket polisdatalagen (1998:622).

Enligt *tredje stycket* gäller lagen inte heller behandling av personuppgifter i vapenregister med stöd av 2 kap. 17–21 §§ vapenlagen (1996:67). Detta hindrar dock inte att det i vapenlagen uttryckligen anges att någon särskild bestämmelse i lagen ska tillämpas på viss behandling. En sådan bestämmelse finns i 2 kap. 22 § vapenlagen.

3 § Följande bestämmelser gäller vid behandling av uppgifter om juridiska personer:

1. 2 kap. 7–9 §§ om ändamålen för behandlingen,
2. 2 kap. 11 § om tillgången till personuppgifter,
3. 2 kap. 12 och 13 §§ om bevarande och gallring,
4. 3 kap. 1–3, 9–12, 14 och 15 §§ om gemensamt tillgängliga uppgifter,
5. 4 kap. 18–20 §§ om behandling av personuppgifter i penningtvättsregister,
6. 4 kap. 21 och 22 §§ om behandling av personuppgifter i det internationella registret,
7. 5 kap. 1–3 §§ om ändamålen för behandlingen hos Säkerhetspolisen,
8. 5 kap. 4 § 5 om tillgången till personuppgifter hos Säkerhetspolisen,

9. 5 kap. 6 och 7 §§ om bevarande och gallring hos Säkerhetspolisen, och

10. 5 kap. 8, 9 och 12–14 §§ om gemensamt tillgängliga uppgifter hos Säkerhetspolisen.

Det som anges om personuppgifter i de angivna paragraferna ska därvid gälla för uppgifter om juridiska personer.

Paragrafen, som i förhållande till 2 § utvidgar lagens tillämpningsområde, innehåller bestämmelser om behandling av uppgifter om juridiska personer. Frågan har behandlats i avsnitt 6.3.

I *första stycket* föreskrivs att vissa av lagens bestämmelser ska tillämpas vid behandling av uppgifter om juridiska personer. Det gäller bestämmelserna om ändamålen med behandlingen (2 kap. 7–9 §§), tillgången till personuppgifter (2 kap. 11 §) och om bevarande och gallring (2 kap. 12 och 13 §§). Det gäller vidare vissa bestämmelser om gemensamt tillgängliga uppgifter (3 kap. 1–3, 9–12 samt 14 och 15 §§) samt om personuppgifter som behandlas i penningtvättsregister (4 kap. 18–20 §§) och i det internationella registret (4 kap. 21 och 22 §§). Motsvarande bestämmelser för Säkerhetspolisens personuppgiftsbehandling (5 kap. 1–3 §§, 4 § 5, 6–9 §§ samt 12–14 §§) ska också tillämpas på juridiska personer.

I *andra stycket* klargörs att vad som anges i de i första stycket uppräknade paragraferna om personuppgifter ska gälla också för uppgifter om juridiska personer.

4 § I 2 kap. finns allmänna bestämmelser om behandling av personuppgifter.

För personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även bestämmelserna i 3 kap.

För personuppgifter som behandlas i register över DNA-profiler, fingeravtrycks- eller signalementsregister, penningtvättsregister eller i det internationella registret, gäller bestämmelser i 4 kap. i stället för bestämmelserna i 3 kap.

I 5 kap. finns bestämmelser om behandlingen av personuppgifter i Säkerhetspolisens verksamhet.

Paragrafen anger hur lagen är uppbyggd.

Första stycket erinrar om att 2 kap. innehåller allmänna bestämmelser om sådan behandling av personuppgifter som lagen reglerar. Bestämmelserna i 2 kap. gäller alltså i princip för all personuppgiftsbehandling som omfattas av lagen (se dock fjärde stycket angående behandling av personuppgifter i Säkerhetspolisens verksamhet).

I *andra stycket* klargörs att det i 3 kap. finns bestämmelser som är tillämpliga vid behandling av personuppgifter ”som görs eller har gjorts gemensamt tillgängliga”. Med detta uttryck avses såväl sådan behandling som innebär att personuppgifterna blir gemensamt tillgängliga som behandling av sådana uppgifter som har blivit gemensamt tillgängliga genom tidigare behandling. Vad som avses med ”gemensamt tillgängliga” behandlas närmare i kommentaren till 3 kap. 1 §. Vid behandling av personuppgifter som omfattas av bestämmelserna i 3 kap. gäller även bestämmelserna i 2 kap.

I *tredje stycket* föreskrivs att vid behandling av personuppgifter i register över DNA-profiler (dvs. DNA-registret, utredningsregistret och spårregistret), fingeravtrycks- eller signalementsregister, penningtvättsregister eller i det internationella registret gäller, utöver bestämmelserna i

2 kap., även vissa bestämmelser i 4 kap. Bestämmelserna i 3 kap. är däremot inte tillämpliga vid sådan behandling.

I *fjärde stycket* anges att bestämmelserna i 5 kap. gäller för behandlingen av personuppgifter i Säkerhetspolisens verksamhet. I 5 kap. anges de bestämmelser i 2–4 kap. som gäller i Säkerhetspolisens verksamhet. Övriga bestämmelser i 2–4 kap. gäller däremot inte för behandling av personuppgifter i den verksamheten.

I vissa bestämmelser i 2–4 kap. anges vilka myndigheter som får ta emot uppgifter som behandlas med stöd av reglerna i kapitlen, t.ex. vilka myndigheter som får beviljas direktåtkomst. I dessa bestämmelser nämns inte Säkerhetspolisen särskilt som mottagare av uppgifter. Säkerhetspolisen kan vara mottagare när Rikspolisstyrelsen anges som mottagande myndighet, eftersom Säkerhetspolisen är en del av Rikspolisstyrelsen. Säkerhetspolisen kan även komma att omfattas när polismyndighet anges som mottagande myndighet, eftersom Säkerhetspolisen för Rikspolisstyrelsens räkning leder viss polisverksamhet och därmed anses som polismyndighet (se 7 § andra stycket polislagen [1984:387] jämförd med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen).

2 kap. Allmänna bestämmelser

Förhållandet till personuppgiftslagen

1 § Om inte annat anges i 2 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

Paragrafen reglerar förhållandet till personuppgiftslagen. Om något annat inte anges i 2 § gäller denna lag i stället för personuppgiftslagen. Vid sådan personuppgiftsbehandling som omfattas av lagen ska alltså bestämmelser i personuppgiftslagen tillämpas endast om det finns en hänvisning till dem i 2 §. Utformningen av den nya lagen skiljer sig i detta avseende från polisdatalagen (1998:622), som gäller utöver personuppgiftslagen. Skälen för detta har utvecklats i avsnitt 6.4.1.

2 § När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 §, med undantag för vad som anges i första stycket i och tredje stycket, om grundläggande krav på behandling,
4. 22 § om behandling av personnummer,
5. 23 och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
12. 48 § om skadestånd, och
13. 51 § första stycket, 52 § första stycket och 53 § om överklagande.

Om personuppgifter ska gallras enligt bestämmelser i denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller inte 8 § andra stycket personuppgiftslagen.

Information enligt 23 § personuppgiftslagen behöver inte lämnas vid behandling som består i insamling av personuppgifter genom bilder eller ljud. Sådan information behöver inte heller lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Paragrafen har kommenterats i avsnitt 6.4.2.

Utgångspunkten är att bestämmelserna i personuppgiftslagen (1998:204) inte ska tillämpas vid sådan behandling av personuppgifter som omfattas av förevarande lag eller föreskrifter som meddelats i anslutning till lagen. Detta följer av 1 §. Vissa utpekade paragrafer i personuppgiftslagen ska dock tillämpas. Dessa anges i *första stycket*. Uppräkningen är uttömmande.

Enligt *punkten 1* ska de definitioner som anges i 3 § personuppgiftslagen tillämpas även vid behandling av personuppgifter som omfattas av förevarande lag.

Genom hänvisningen i *punkten 2* till 8 § personuppgiftslagen klargörs att bestämmelserna i förevarande lag – eller de bestämmelser till vilka lagen hänvisar – inte ska tillämpas om det skulle inskränka polisens skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter (jfr 8 § första stycket personuppgiftslagen). Det innebär t.ex. att en myndighet inte kan vägra att ta fram och lämna ut uppgifter i enlighet med tryckfrihetsförordningens bestämmelser enbart med hänvisning till att utlämnandet inte ryms inom de i 7–9 §§ angivna ändamålen för behandling. I sammanhanget bör dock understrykas att offentlighetsprincipen inte innebär någon skyldighet att lämna ut uppgifter i elektronisk form. Vid bedömningen av om en uppgift kan lämnas ut i elektronisk form måste alltså lagens regler beaktas.

Av hänvisningen till 8 § personuppgiftslagen följer också att förevarande lag inte hindrar att en myndighet arkiverar eller bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (jfr 8 § andra stycket personuppgiftslagen). Bestämmelserna om gallring i förevarande lag gäller dock framför bestämmelsen i 8 § andra stycket. Detta följer av paragrafens andra stycke.

Vidare hänvisas i *punkten 3* till 9 § personuppgiftslagen, med undantag för första stycket i och tredje stycket. Hänvisningen innebär att den personuppgiftsansvarige (jfr 4 §) ska se till att uppgifterna behandlas enbart om det är lagligt och att de behandlas på ett korrekt sätt och i enlighet med god sed. I förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 143) uttalas att vad som är god sed vid behandling av personuppgifter får avgöras i rättstillämpningen mot bakgrund av bl.a. de mer preciserade föreskrifter som kan utfärdas med stöd av personuppgiftslagen, de branschregler på området som kan ha utarbetats av etablerade branschorganisationer eller andra representativa sammanslutningar och hur ansvarsfulla personuppgiftsansvariga som regel beter sig.

Den personuppgiftsansvarige ska också se till *dels* att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen

för behandlingen, *dels* att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen, *dels* att de behandlade personuppgifterna är riktiga och, om det är nödvändigt, aktuella, *dels* att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Det är givet att man vid tillämpningen av de aktuella bestämmelserna måste ta hänsyn till den särskilda karaktären hos de uppgifter som förekommer i brottsbekämpande verksamhet. Exempelvis kan kravet på att de behandlade uppgifterna är riktiga inte anses innebära något hinder mot att samla in osäkra underrättelseuppgifter, under förutsättning att uppgifterna har relevans för underrättelsearbetet och att det framgår att uppgiftens riktighet är osäker (se kommentaren till 3 kap. 4 § andra stycket). Hänvisningen innebär vidare att den personuppgiftsansvarige ska se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål och att personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (den s.k. finalitetsprincipen).

Vidare hänvisas i *punkten 4* till 22 § personuppgiftslagen. Bestämmelsen innebär att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke i polisens brottsbekämpande verksamhet bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Av hänvisningen i *punkten 5* till 23 § personuppgiftslagen följer att den myndighet som samlar in uppgifter om en enskild person från personen själv självmant ska informera honom eller henne om behandlingen. Det innebär t.ex. att en polismyndighet i samband med att den tar emot och behandlar en uppgift från en person om att denne har utsatts för brott ska underrätta honom eller henne om behandlingen. I 25 § personuppgiftslagen anges att informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, uppgift om ändamålen med behandlingen samt övrig information som den aktuella personen behöver för att ta till vara sina rättigheter i samband med behandlingen av uppgifterna.

Bestämmelserna om informationsplikt i 23 och 25 §§ personuppgiftslagen modifieras emellertid av andra bestämmelser. Som framgår av hänvisningen till 27 § personuppgiftslagen gäller informationsplikten inte i den utsträckning det råder sekretess eller tystnadsplikt för informationen. Som en följd av detta gäller t.ex. ingen informationsplikt när en polis som arbetar under skyddsidentitet samlar in uppgifter från misstänkta, eftersom informationsinhämtandet i den situationen torde skyddas av sekretess enligt 18 kap. 1, 2, 5 eller 6 § offentlighets- och sekretesslagen (2009:400). Informationsskyldigheten begränsas också av de särskilda bestämmelserna i tredje stycket.

Som framgår av hänvisningen till 26 § personuppgiftslagen är den personuppgiftsansvarige skyldig att på begäran lämna information till en sökande om huruvida personuppgifter som rör denne behandlas. Om sådan behandling sker, ska upplysning också lämnas om bl.a. ändamålet med behandlingen. Också denna informationsskyldighet modifieras genom bestämmelserna i 27 § personuppgiftslagen. Om det gäller sekretess för uppgiften behöver någon information inte lämnas. Det innebär t.ex.

att information inte behöver lämnas om sådant som polisen har inhämtat i sin underrättelseverksamhet, om det kan antas att syftet med beslutade eller förutsedda åtgärder skulle motverkas av att information lämnas (18 kap. 2 § offentlighets- och sekretesslagen).

Enligt hänvisningen i *punkten 6* till 28 § personuppgiftslagen ska också den lagens bestämmelser om rättelse tillämpas. Den personuppgiftsansvarige är alltså skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med förevarande lag – däribland de bestämmelser i personuppgiftslagen till vilka lagen hänvisar – eller föreskrifter som har utfärdats i anslutning till lagen. Rättelse ska dock inte ske enbart därför att uppgifter som framstod som riktiga eller rimliga när de samlades in, t.ex. brottsmisstankar, senare har visat sig vara oriktiga.

I *punkten 7* görs en hänvisning till 30 och 31 §§ samt 32 § första stycket personuppgiftslagen. Enligt 30 § första stycket får ett personuppgiftsbiträde (dvs. den som behandlar personuppgifter för den personuppgiftsansvariges räkning) och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning behandla personuppgifter enbart 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, gäller dock – enligt 30 § tredje stycket – dessa i stället. Den sistnämnda bestämmelsen syftar särskilt på bestämmelser om tystnadsplikt och sekretess (se prop. 1997/98:44 s. 136). Av 31 § följer bl.a. att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de behandlade personuppgifterna. Enligt 32 § första stycket får tillsynsmyndigheten i enskilda fall besluta om vilka åtgärder som den personuppgiftsansvarige ska vidta enligt 31 §. Med tillsynsmyndigheten avses här tillsynsmyndigheten enligt personuppgiftslagen, dvs. Datainspektionen (2 § personuppgiftsförordningen [1998:1191]).

En hänvisning görs i *punkten 8* till 33–35 §§ personuppgiftslagen. Enligt 33 § är det förbjudet att överföra personuppgifter till tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifter. Frågan om en skyddsnivå är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska fästas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och reglerna för behandlingen i tredjeland. I 34 och 35 §§ föreskrivs undantag från förbudet. Enligt 34 § får uppgifter trots förbudet överföras dels om den registrerade har lämnat sitt samtycke till överföringen, dels om överföringen är nödvändig med hänsyn till vissa uppräknade omständigheter. Det är också enligt den paragrafen tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. I 35 § föreskrivs att regeringen, och för vissa fall även den myndighet som regeringen bestämmer, får meddela föreskrifter om undantag från förbudet i 33 §.

I *punkten 9* görs en hänvisning till 38–40 §§ personuppgiftslagen, där det framgår vilka närmare uppgifter ett personuppgiftsombud har. Jfr 5 § angående skyldigheten att utse personuppgiftsombud. En hänvisning görs också till 41 § personuppgiftslagen. Enligt den paragrafen har regeringen

möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll.

Hänvisningen i *punkten 10* till 42 § personuppgiftslagen innebär att den personuppgiftsansvarige ska till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten, dvs. Datainspektionen. Sekretessbelagda uppgifter och uppgifter om vidtagna säkerhetsåtgärder behöver dock inte lämnas ut.

Datainspektionen har rätt att för sin tillsyn på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Detta framgår av hänvisningen i *punkten 11* till 43 § personuppgiftslagen. Om inspektionen inte har tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får den med stöd av hänvisningen till 44 § personuppgiftslagen förbjuda behandlingen. Konstaterar Datainspektionen att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska inspektionen genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Om det inte går att få till stånd rättelse, eller om saken är brådskande, får Datainspektionen förbjuda behandlingen, vilket följer av hänvisningen till 45 § första stycket personuppgiftslagen. Vidare hänvisas till 47 § personuppgiftslagen där Datainspektionen ges rätt att hos länsrätten ansöka om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

Som framgår av hänvisningen i 6 § till lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet utövar även Säkerhets- och integritetsskyddsnämnden viss tillsyn över polisens personuppgiftsbehandling. Nämndens befogenheter regleras i den lagen. Frågor om tillsyn har behandlats i avsnitt 17.2.

Av hänvisningen i *punkten 12* till 48 § personuppgiftslagen följer att den personuppgiftsansvarige ska ersätta den registrerade för sådan skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med förevarande lag – och de bestämmelser i personuppgiftslagen till vilka lagen hänvisar – har orsakat.

Av hänvisningen i *punkten 13* till 51 § första stycket personuppgiftslagen följer att Datainspektionens beslut får överklagas till allmän förvaltningsdomstol. Som framgår av hänvisningen till 52 § första stycket personuppgiftslagen kan den personuppgiftsansvariga myndighetens beslut om information enligt 26 §, om rättelse och om underrättelse till tredje man enligt 28 § och om upplysningar enligt 42 § personuppgiftslagen också överklagas hos allmän förvaltningsdomstol. Av hänvisningen till 53 § personuppgiftslagen följer att andra beslut inte får överklagas.

I *andra stycket* regleras hur gallringsregler i lagen, och i föreskrifter som meddelats i anslutning till lagen, förhåller sig till hänvisningen i första stycket punkten 2. Bestämmelsen innebär att denna lag ges företräde framför bestämmelserna i 8 § andra stycket personuppgiftslagen.

Det *tredje stycket* innehåller två undantag från informationsskyldigheten i 23 § personuppgiftslagen. För det första behöver information inte lämnas om uppgifterna samlas in genom bild- eller ljudupptagning. Undantaget omfattar bl.a. insamling genom hemlig teleavlyssning, hemlig rumsavlyssning och hemlig kameraövervakning enligt bestämmelser i

rättegångsbalken, lagen (1998:150) om allmän kameraövervakning, lagen (2007:978) om hemlig rumsavlyssning, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott. Särskilda bestämmelser om tvångsmedelsanvändning som omfattas av undantaget finns dessutom i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Vidare omfattas fotografering som sker med stöd 28 kap. 14 § rättegångsbalken av undantaget från informationsskyldigheten. Även insamling genom bild- och ljudupptagning som inte är författningsreglerad omfattas av undantaget.

För det andra behöver information enligt 23 § inte lämnas om uppgifterna samlas in i samband med ett larm och det med hänsyn till omständigheterna inte finns tid att lämna information. Med larm avses en brådskande begäran om att polisen omedelbart ska vidta en åtgärd av något slag. Larm görs vanligtvis till polisens kommunikationscentraler, men bestämmelsen tar sikte även på de situationer där en person vänder sig till en enskild polisman eller till en telefonist i polisens allmänna växel. I sådan verksamhet som består av att ta emot larm, t.ex. vid en kommunikationscentral, torde information enligt 23 § aldrig behöva lämnas, eftersom det i den verksamheten typiskt sett inte finns tid att lämna information. När larm görs i andra sammanhang, måste det avgöras från fall till fall om det finns tid att lämna informationen. Avgörande för denna bedömning bör främst vara om det skulle medföra en försening av den efterfrågade åtgärden eller om åtgärden på annat sätt skulle påverkas negativt av att informationen lämnas. Om undantaget från informationsplikten är tillämpligt, behöver polisen inte heller lämna informationen i efterhand.

Förbud enligt 44 eller 45 § personuppgiftslagen får normalt förenas med vite. I *fjärde stycket* föreskrivs dock att förbud som meddelas i samband med tillsyn enligt denna lag inte får förenas med vite.

Definition av DNA-analys, DNA-profil och fingeravtryck

3 § I denna lag avses med

DNA-analys:	varje förfarande som kan användas för analys av deoxyribonukleinsyra i humant material,
DNA-profil:	resultatet av en DNA-analys som presenteras i form av siffror eller bokstäver, och
fingeravtryck:	fingeravtryck eller handavtryck.

I paragrafen definieras begreppen DNA-analys, DNA-profil och fingeravtryck. I förhållande till definitionen av DNA-analys i 3 § polisdatalagen (1998:622) har ett tillägg gjorts för att tydliggöra att regleringen enbart omfattar DNA-analys av prov från en människa. Vid en DNA-analys undersöks en liten del av arvsmassan i syfte att få fram för individen unika identifikationsuppgifter.

I polisdatalagen finns ingen definition av DNA-profil. I stället för DNA-profil används uttrycket ”uppgifter om resultatet av DNA-analyser”. En DNA-profil består av uppgifter som har tagits fram med hjälp av DNA-analys, dvs. analys av deoxyribonukleinsyra i antingen ett särskilt

prov från humant biologiskt material (t.ex. blod, hår eller hudceller) eller från spår som innehåller sådant material och som har påträffats på eller i nära anslutning till en brottsplats. En DNA-profil får enbart presenteras i form av siffror eller bokstäver eller en kombination av siffror och bokstäver. Därmed går det inte att identifiera en person enbart med stöd av DNA-profilen. Bakgrunden till att det införs en definition av begreppet DNA-profil har beskrivits i avsnitt 9.6.

I paragrafen definieras även vad som avses med fingeravtryck. Definitionen motsvarar vad som registreras för närvarande, dvs. avtryck av fingrar eller hand. Definitionen uppfyller kraven i Prümrådsbeslutet (se avsnitt 15.3).

Personuppgiftsansvar

4 § Rikspolisstyrelsen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför och den behandling som utförs i polisens verksamhet vid Ekobrottsmyndigheten. Var och en av polismyndigheterna är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Frågan har behandlats i avsnitt 6.5.

I paragrafen anges att Rikspolisstyrelsen och var och en av polismyndigheterna är personuppgiftsansvariga för den behandling av personuppgifter enligt 1–4 kap. som respektive myndighet utför. Av 5 kap. 5 § framgår att Säkerhetspolisen på motsvarande sätt är personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför.

Enligt 1 kap. 2 § första stycket är lagen tillämplig på polisens brottsbekämpande verksamhet vid Ekobrottsmyndigheten. Den polispersonal som arbetar vid Ekobrottsmyndigheten är tillkallad av Rikspolisstyrelsen; se 8 § förordningen (1989:773) med instruktion för Rikspolisstyrelsen och 7 § förordningen (2007:972) med instruktion för Ekobrottsmyndigheten. Rikspolisstyrelsen leder sådan verksamhet vid Ekobrottsmyndigheten som enligt lag eller annan författning endast får utföras av anställda inom polisen (6 § 7 instruktionen för Rikspolisstyrelsen). Styrelsen är enligt förevarande paragraf personuppgiftsansvarig för den personuppgiftsbehandling som sker i den brottsbekämpande verksamhet som bedrivs av polispersonal vid Ekobrottsmyndigheten.

Uttrycket personuppgiftsansvarig definieras i 3 § personuppgiftslagen (1998:204). Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Flera bestämmelser i personuppgiftslagen, till vilka det hänvisas i 2 §, ålägger den personuppgiftsansvarige särskilda skyldigheter. Så är det t.ex. enligt 9 § första stycket personuppgiftslagen den personuppgiftsansvariges skyldighet att se till att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen för behandlingen och att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen. Det ankommer också på den personuppgiftsansvarige att se till att information lämnas till den registrerade och att uppgifter gallras i rätt tid.

Den myndighet som samlar in och lagrar personuppgifter är personuppgiftsansvarig för den behandlingen. Om samma uppgift lämnas ut till

en annan myndighet, genom direktåtkomst eller på annat sätt, blir den mottagande myndigheten personuppgiftsansvarig för den fortsatta behandlingen av uppgiften hos den myndigheten. När uppgifter lämnas ut till olika myndigheter kan alltså personuppgiftsansvaret för en och samma uppgift komma att ligga hos flera myndigheter. Var och en av dessa ansvarar för den egna behandlingen.

5 § Rikspolisstyrelsen och var och en av polismyndigheterna ska utse ett eller flera personuppgiftsombud.

Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Frågan har kommenterats i avsnitt 6.5.

I *första stycket* föreskrivs att Rikspolisstyrelsen och var och en av polismyndigheterna ska utse ett eller flera personuppgiftsombud. Hänvisningen i 2 § första stycket 9 till 38–40 §§ personuppgiftslagen (1998:204) innebär att den lagens bestämmelser om personuppgiftsombudets uppgifter blir tillämpliga vid Rikspolisstyrelsen och polismyndigheterna.

Som framgår av kommentaren till 4 § är Rikspolisstyrelsen personuppgiftsansvarig för den personuppgiftsbehandling som sker i den brottsbekämpande verksamhet som bedrivs av polispersonal vid Ekobrottsmyndigheten. Personal anställd vid Ekobrottsmyndigheten bör inte utses till personuppgiftsombud för sådan behandling.

Enligt *andra stycket* ska den personuppgiftsansvarige anmäla till tillsynsmyndigheten enligt personuppgiftslagen, dvs. Datainspektionen, när ett personuppgiftsombud utses eller entledigas. En motsvarande bestämmelse finns i 36 § andra stycket personuppgiftslagen.

Tillsyn

6 § Ytterligare bestämmelser om tillsyn finns i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Paragrafen innehåller en erinran om den tillsyn som Säkerhets- och integritetsskyddsnämnden ska utöva över polisens personuppgiftsbehandling. Frågan har behandlats i avsnitt 17.2.

Ändamål

7 § Personuppgifter får behandlas om det behövs för att
1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller beivra brott, eller
3. fullgöra de förpliktelser som följer av internationella åtaganden.

Paragrafen anger de *primära ändamål* för vilka personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Avgränsningen av dessa ändamål har behandlats i avsnitt 7.2–7.4. Personuppgifter får också behandlas för planering, uppföljning och utvärdering av polisens brottsbekämpande verksamhet. Sådan behandling anses utgöra en del av själva verksamheten och behöver inte regleras särskilt (prop. 2004/05:164

s. 179). Personuppgifter som behandlas med stöd av 7 § får också behandlas för ett antal ytterligare ändamål. Behandlingen för dessa *sekundära ändamål* regleras i 8 §. Av 9 § framgår att personuppgiftsbehandling dessutom får ske för diarieföring och inom ramen för viss ärendehantering. Vidare får personuppgifter behandlas för ett nytt ändamål, om det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in. Ramarna för sådan vidarebehandling sätts av den s.k. finalitetsprincipen, se hänvisningen i 2 § första stycket punkten 3 till 9 § första stycket d personuppgiftslagen (1998:204). Som framgår av hänvisningen i 2 § första stycket punkten 2 till 8 § personuppgiftslagen får behandling också ske i den mån den är nödvändig för att polisen ska kunna fullgöra sina skyldigheter enligt 2 kap. tryckfrihetsförordningen. Tillsammans avgränsar de nu nämnda paragraferna för vilka ändamål behandling av personuppgifter är tillåten i polisens brottsbekämpande verksamhet. Lagens ändamålsreglering har behandlats i avsnitt 7.1.

En grundläggande förutsättning för att en personuppgift ska få behandlas med stöd av 7 § är att den behövs för viss särskilt angiven polisiär verksamhet. Med detta avses att det ska finnas ett konkret behov av att genomföra behandlingen och att detta behov svarar mot ändamålet med denna. Som exempel kan nämnas att det i en förundersökning kan vara nödvändigt att sammanställa uppgifter om vilka personer som har befunnit sig på platsen för brottet för att säkerställa att alla presumtiva vittnen har hörts i saken, att sammanställa en förteckning över alla målsägande och deras ersättningskrav eller att redovisa vilka personer som har haft kontakt med ett offer i tidsmässigt nära samband med brottet. Likaså måste självfallet många personuppgifter om misstänkta behandlas för att tillgodose dels åklagarens behov av underlag för sitt ställningstagande i åtalsfrågan, dels domstolens behov av personutredning i brottmål (jfr bestämmelserna i 20 och 21 §§ förundersökningskungörelsen [1947:948] om vad ett förundersökningsprotokoll ska innehålla). Om ändamålet med personuppgiftsbehandlingen är att förebygga eller förhindra brott, kan det t.ex. vara nödvändigt att sammanställa uppgifter om vem som hyr vissa lokaler eller vem som äger eller disponerar fordon som man misstänker används i den brottsliga verksamheten. Det kan också handla om att klarlägga vilka personer som regelbundet besöker en viss plats där man misstänker att allvarlig brottslig verksamhet förekommer. Som exempel på att en viss behandling normalt inte behövs kan nämnas att det i en förundersökning om ekonomisk brottslighet rimligen inte behövs behandling av uppgifter om att den misstänkte tidigare har varit misstänkt för eller dömts för sexualbrott. I underrättelseprojekt som rör en viss typ av allvarlig brottslighet bör inte underrättelseuppgifter som helt saknar samband med just det aktuella projektet få behandlas. Är uppgifterna av annat skäl av intresse för brottsbekämpningen, får de i stället behandlas inom ramen för en annan förundersökning eller ett annat underrättelseprojekt.

En stor mängd av den information som polisen samlar in och bearbetar för ett specifikt ändamål, exempelvis för att utreda ett visst brott, måste kunna vidarebehandlas för andra ändamål som antingen anknyter till det ursprungliga ändamålet eller ligger vid sidan av detta. Sådan vidarebehandling är tillåten, under förutsättning att den efterföljande behandlingen faller in under något av ändamålen i 7–9 §§ eller om det efter en

prövning i det enskilda fallet bedöms att vidarebehandlingen inte kan anses oförenlig med insamlingsändamålet (finalitetsprincipen).

I *punkten 1* anges att personuppgifter får behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet (avsnitt 7.2). Det polisarbete som åsyftas är framför allt det som vanligtvis kallas underrättelseverksamhet, dvs. arbete med insamling, bearbetning och analys av information för att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § andra stycket rättegångsbalken omfattas av denna punkt, om syftet är att förhindra brott. Polisarbete som är inriktat på en redan begången individualiserad brottslig gärning faller in under punkten 2.

Av *punkten 2* framgår att personuppgifter får behandlas för att utreda eller beivra brott (avsnitt 7.3). Huvuddelen av polisens verksamhet under denna punkt består av förundersökning eller annan utredning enligt bestämmelserna i 23 kap. rättegångsbalken, men polisen har även vissa uppgifter som avser beivrande av brott. Under beivrande av brott faller främst föreläggande av ordningsbot men även biträde till åklagare t.ex. i ärenden om ändrad påföljd.

Med brott avses ett konkret brott. 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. Om misstankarna enbart gäller icke-preciserad brottslighet, är det dock i stället fråga om sådan ”brottslig verksamhet” som avses i punkten 1. Rör misstanken ett visst brott som kan komma att begås i framtiden kan personuppgiftsbehandling vara tillåten med stöd av punkten 1. Har den förväntade gärningen nått den punkt där den är straffbar såsom försök, förberedelse, stämpling eller anstiftan – dvs. om det finns grund för att inleda förundersökning – är det däremot fråga om personuppgiftsbehandling som sker med stöd av punkten 2.

Under punkten 2 faller all personuppgiftsbehandling inom ramen för en förundersökning (även spaning). Detsamma gäller behandling av personuppgifter med stöd av 23 kap. 3 och 8 §§ rättegångsbalken innan en förundersökning har inletts och behandling inom ramen för en s.k. förenklad utredning enligt 23 kap. 22 § rättegångsbalken. Handläggningen av en brottsanmälan hör också hit, även om denna inte leder till något beslut om att inleda förundersökning.

Punkten 2 är också tillämplig vid sådan utredning som inte utgör förundersökning men som polisen utför, för egen räkning eller åt åklagare, med stöd av lag eller annan författning enligt reglerna i 23 kap. rättegångsbalken om förundersökning. Exempel på sådana bestämmelser finns i 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, 16 § lagen (1957:668) om utlämning för brott, 10 § lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge, 9 § lagen (1988:688) om besöksförbud, 4 kap. 3 § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder och 8 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang.

Punkterna 1 och 2 avser endast brottsbekämpande verksamhet som bedrivs av svensk polis för dess egna intressen. Av *punkten 3* följer att behandling av personuppgifter i vissa fall får ske, om syftet är att gagna

utländsk brottsbekämpande verksamhet (avsnitt 7.4). I den mån ett internationellt åtagande innebär att svensk polis är skyldig att fullgöra vissa förpliktelser och den konkreta arbetsuppgiften kräver att polisen ska kunna behandla personuppgifter, är behandlingen tillåten enligt denna punkt. Detta gäller oavsett om den brottslighet som den utländska brottsbekämpande verksamheten avser faller in under svensk jurisdiktion eller inte. Sådana förpliktelser kan följa dels av vissa lagar som genomför internationella överenskommelser och som reglerar viss polisverksamhet, dels direkt av vissa internationella överenskommelser.

Till de lagar som innehåller förpliktelser av detta slag hör lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar. Den reglerar polisiärt samarbete mellan EU:s medlemsstater och innehåller bl.a. bestämmelser om gemensamma utredningsgrupper och om uppgifter och bevisning som lämnas till en sådan grupp. En annan sådan lag är lagen (2000:343) om internationellt polisiärt samarbete, som reglerar operativt polisiärt samarbete bl.a. inom EU. Som framgår av 1 kap. 2 § andra stycket faller däremot behandling av personuppgifter som sker med stöd av lagen (2000:344) om Schengens informationssystem utanför denna lags tillämpningsområde. Sådan brottsutredning som sker inom ramen för rättslig hjälp till en annan stat hör också hemma under punkten 3, om den inte faller under punkten 2.

Som exempel på situationer där punkten 3 kan bli tillämplig kan nämnas att Sverige i flera internationella överenskommelser har åtagit sig att inom polisen ha en nationell kontaktpunkt som myndigheter i andra länder kan nå dygnet runt, året om. En sådan kontaktpunkt ska bl.a. kunna ta emot och lagra information samt besvara förfrågningar av olika slag. Detta kräver i många fall personuppgiftsbehandling. Ett annat exempel är när polisen i ett ärende om rättslig hjälp vidtar utredningsåtgärder för en utländsk polismyndighets räkning, genom t.ex. verkställighet av tvångsmedel. Det kan också vara fråga om en skyldighet att underrätta en främmande stats konsulat eller beskickning om att någon av statens medborgare har berövats friheten i Sverige.

Sådan personuppgiftsbehandling som utförs av polisen i syfte att lämna ut redan insamlad information till andra kan också ske med stöd av lagens sekundära ändamål (se avsnitt 7.6 och kommentaren till 8 §).

8 § Personuppgifter som behandlas enligt 7 §, får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,
3. sådan verksamhet hos polisen som avser handräckningsuppdrag,
4. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen,
5. verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten, eller
6. en myndighets verksamhet

a) om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift, eller

b) om tillhandahållandet görs i syfte att samverka mot brott.

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

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 7 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter och att uppgifter som behandlas i en förundersökning får tillhandahållas konkursförvaltare.

I paragrafen anges de *sekundära ändamål* för vilka personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Frågan har behandlats i avsnitt 7.6. Behandling av personuppgifter enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling enligt 7 §. Det är alltså inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem enligt denna paragraf. Utgångspunkten är att de angivna sekundära ändamålen i allt väsentligt ska täcka in det utlämnande som kan komma i fråga. För att behandling för andra ändamål än de i paragrafen uppräknade ska vara tillåten krävs att den inte kan anses oförenlig med insamlingsändamålet (finalitetsprincipen). Det förhållandet att uppgifter i vissa fall får behandlas för utlämnande av information påverkar inte de bestämmelser som gäller om sekretess. Bestämmelserna i offentlighets- och sekretesslagen (2009:400) om sekretess mellan och inom myndigheter liksom bestämmelser i andra författningar som bryter sekretess ska således beaktas på vanligt sätt. I kommentaren till 14–19 §§ behandlas de sekretessbrytande bestämmelserna i denna lag.

I sammanhanget bör också framhållas att polisen kan lämna ut personuppgifter med stöd av 7 §, om åtgärden är ett led i den egna verksamheten. Som exempel kan nämnas att polisen i en svensk förundersökning kan begära rättslig hjälp av t.ex. en utländsk myndighet och i samband med detta tillhandahålla nödvändig information med stöd av 7 § 2.

Av *första stycket punkten 1* framgår att personuppgifter som behandlas med stöd av 7 § även får behandlas för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket. I detta sammanhang nämns även Rikspolisstyrelsen, polismyndigheter och Ekobrottsmyndigheten. Därmed klargörs att uppgifter får behandlas för att tillhandahållas andra myndigheter som omfattas av lagens tillämpningsområde. Rikspolisstyrelsen får t.ex. behandla uppgifter för att tillhandahålla information till en annan polismyndighet. Vad gäller Ekobrottsmyndigheten innebär bestämmelsen att uppgifter kan tillhandahållas även åklagare vid myndigheten.

Med polismyndighet avses även Säkerhetspolisen när man där för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet (se 7 § andra stycket polislagen [1984:387] jämförd med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen). När Säkerhetspolisen utför andra uppgifter (3 § instruktionen) är den en del av Rikspolisstyrelsen. Uppgifter som behandlas hos den övriga polisen kan således tillhandahållas Säkerhetspolisen med stöd av första punkten.

Punkten 2 ger möjlighet att behandla personuppgifter som behandlas enligt 7 § för att tillhandahålla en utländsk myndighet eller mellanfolklig

organisation den information som behövs i dess brottsbekämpande verksamhet. Denna bestämmelse ger stöd för själva behandlingen av uppgifterna. Hur stort utrymmet är för utlämnande av uppgifter bestäms som nyss nämnts av reglerna om sekretess, se kommentaren till 15 §. De utländska myndigheter som avses i punkt 2 är främst polis- och åklagarmyndigheter. I den mån brottsbekämpande verksamhet handhas av någon annan myndighet ger dock denna punkt utrymme för att tillhandahålla personuppgifter även till den myndigheten. Det kan t.ex. vara fråga om specialmyndigheter med brottsbekämpande uppgifter på det finansiella området. Möjligheten att behandla uppgifterna genom att lämna ut dem kan begränsas av reglerna i 33–35 §§ personuppgiftslagen (1998:204), som inskränker möjligheten att överföra uppgifter till tredjeland (jfr kommentaren till 2 § första stycket 8).

Enligt *punkten 3* får personuppgifter som behandlas med stöd av 7 § även behandlas om det är nödvändigt för att tillhandahålla information som behövs när polisen bistår andra myndigheter med handräckningsuppdrag. Uppgifter som finns i uppgiftssamlingar i den brottsbekämpande verksamheten får således tillhandahållas polisen inför ett sådant uppdrag för att polisen på bästa sätt ska kunna förbereda sig för uppdraget. Det kan t.ex. vara fråga om uppgift om att en person har gjort våldsamt motstånd eller varit beväpnad vid verkställighet av straffprocessuella tvångsmedel, eller uppgifter om hos vem personen brukar vistas.

Punkten 4 tar sikte på behandling av personuppgifter för att tillhandahålla uppgifter till sådan polisär verksamhet som inte är brottsbekämpande och som inte heller avser handräckningsuppdrag. Om den som handlägger t.ex. ett förvaltningsärende begär att få information, ska den alltid lämnas med stöd av 6 kap. 5 § offentlighets- och sekretesslagen om sekretess inte hindrar det (se paragrafens andra stycke). Det kan t.ex. röra sig om att få en uppgift i belastningsregistret eller misstankeregistret närmare belyst genom att ta del av uppgifter i en förundersökning. Punkten ger polisen ett visst utrymme att spontant överlämna personuppgifter som har samlats in med stöd av 7 § för användning i olika förvaltningsärenden hos polisen, t.ex. vapenärenden. En förutsättning för behandling enligt denna punkt är dock att det finns särskilda skäl att tillhandahålla informationen. Informationen får alltså inte rutinmässigt tillhandahållas för annan polisiär verksamhet, utan det måste i det enskilda fallet finnas särskilda omständigheter som talar för att informationen bör överlämnas.

Ett fall där bestämmelsen torde kunna tillämpas är om det genom underrättelseinformation har kommit fram att en viss person har täta kontakter med andra personer som kan antas ägna sig åt organiserad brottslighet i någon form. Om den förstnämnde begär olika typer av tillstånd till verksamhet kan det, med anledning av underrättelseinformationen, finnas skäl att närmare undersöka om denne kan vara bulvan för de senare och om tillstånd trots detta bör beviljas. Det är då viktigt att informationen kommer handläggaren till del. I ärenden om tillstånd till offentlig tillställning och liknande ärenden kan det också ibland vara befogat att tillföra ärendet uppgifter av underrättelsekaraktär, särskilt när det kan antas att det kan komma att begås allvarlig brottslighet i samband med evenemanget.

Punkten 5 ger möjlighet att behandla personuppgifter som behandlas enligt 7 § för att tillhandahålla Kriminalvården sådan information som myndigheten behöver i sin verksamhet för att förebygga brott och upprätthålla säkerheten. Enligt 2 § förordningen (2007:1172) med instruktion för Kriminalvården har myndigheten bl.a. till uppgift att verka för att påföljder verkställs på ett säkert sätt och att återfall i brott förebyggs. I detta arbete har myndigheten ibland behov av att få del av information från polisens brottsbekämpande verksamhet. Sådan information kan bl.a. vara av avgörande betydelse inför beslut om placering på anstalt eller transport av personer, t.ex. uppgifter om koppling till andra personer som avtjänar straff eller koppling till viss organiserad brottslighet. Information från polisen kan även vara betydelsefull i ärenden om tillstånd att ta emot besök och telefonsamtal samt vid planering av permissioner. Som nämnts inledningsvis i kommentaren till denna paragraf påverkar inte det förhållandet att uppgifter får behandlas enligt denna paragraf de bestämmelser som gäller om sekretess. Ett utlämnande måste således föregås av en sedvanlig sekretessprövning.

Punkten 6 a är avsedd att tillgodose polisens i författning reglerade åligganden att biträda en annan svensk myndighet i dess verksamhet. Denna punkt täcker bl.a. den behandling som kan krävas för att polisen ska kunna bistå Riksdagens ombudsmän och Justitiekanslern med uppgifter när de uppträder som förundersökningsledare och åklagare, i den mån det inte är fråga om en behandling som faller in under 7 § 2. Enligt 6 kap. 20 § tullagen (2000:1281) har polisen även rätt att vidta olika åtgärder som normalt utförs av tulltjänstemän (bl.a. att inom ramen för en tullkontroll anbringa lås eller omhänderta handlingar). Denna punkt ger således polisen rätt att behandla personuppgifter inom ramen för biträde i sådan verksamhet.

Punkten 6 b ger polisen möjlighet att behandla personuppgifter för att tillhandahålla information till svenska myndigheter i syfte att samverka mot brott. Det rör sig om tillhandahållande av uppgifter till myndigheter som inte har till uppgift att bekämpa brott, men där tillhandahållandet är till nytta för polisens brottsbekämpande verksamhet. Syftet med paragrafen är att möjliggöra tillhandahållande inom ramen för myndighetsövergripande samverkan mot brott, t.ex. arbetet i ett regionalt underrättelsecentrum. Det kan vara fråga om såväl strategiskt som operativt samarbete, t.ex. i gemensamma operationer för att förhindra viss typ av brottslighet. Ett annat exempel på sådan samverkan, där syftet inte enbart är brottsbekämpande, är Operation krogsanering i Stockholm. Detta är ett samverkansprojekt mellan bl.a. länsstyrelsen, polisen, Skatteverket, Migrationsverket, kommunernas tillståndsenheter och Ekobrottsmyndigheten. Syftet med projektet är att kontrollera att näringsidkare följer gällande tillstånd och regelverk. Tillhandahållande av personuppgifter till en myndighet i ett enskilt ärende, t.ex. gällande tillstånd eller bidrag, omfattas normalt inte av samverkan mot brott enligt denna bestämmelse. Sådant tillhandahållande kan dock omfattas, om det utgör en del av ett större, planlagt samarbete mellan polisen och myndigheten för visst närmare preciserat brottsbekämpande ändamål. Som tidigare nämnts krävs en sedvanlig sekretessprövning innan uppgifter lämnas ut.

I *andra stycket* anges att personuppgifter får behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen

samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till annan. Med annan avses såväl myndighet som enskild. Exempel på uppgiftsskyldighet gentemot annan myndighet finns i 14 kap. 1 § socialtjänstlagen (2001:453) som föreskriver skyldighet att göra anmälan till socialnämnden när nämnden behöver ingripa till barns skydd. I vissa fall är polisen skyldig att avge yttrande till annan myndighet med skyldighet att redovisa viss information eller grunden för sitt ställningstagande. Också detta utgör en skyldighet som omfattas av den aktuella bestämmelsen. Som exempel kan nämnas polismyndighetens yttrande till en kommun i ärenden om tillstånd till alkoholutskänkning (7 kap. 14 § alkohollagen [1994:1738]). Andra exempel på skyldighet att lämna uppgifter som kan omfatta även polisen finns i 12 kap. 6 § regeringsformen och 6 § lagen (2002:1022) om revision av statlig verksamhet m.m. där det föreskrivs skyldighet att tillhandahålla Riksdagens ombudsmän respektive Riksrevisionen begärda upplysningar. Vidare omfattas en myndighets skyldighet enligt 6 kap. 5 § offentlighets- och sekretesslagen att på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång.

Enligt 17 § polisdataförordningen (1999:81) får uppgifter om efterlysta personer och om avlägsnanden ur landet lämnas till vissa myndigheter. Vidare får, enligt 17 a § samma förordning, förundersökningsuppgifter som kan antas ha betydelse för en konkursutredning lämnas till konkursförvaltaren. I *tredje stycket* finns en upplysning om att regeringen kan meddela föreskrifter om motsvarande tillhandahållande av personuppgifter. Se även kommentaren till 19 §.

9 § Personuppgifter får behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Paragrafen reglerar behandling av personuppgifter i två speciella fall och gäller oavsett om förutsättningarna för behandling enligt 7 eller 8 § är för handen. Frågan har berörts i avsnitt 7.5.

Enligt *punkten 1* får personuppgifter alltid behandlas om behandlingen är nödvändig för diarieföring. 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 således alltid anges vem handlingen har kommit från och i korthet vad handlingen rör. Någon annan behandling än sådan som är nödvändig för diarieföringen får emellertid inte ske med stöd av första punkten. Den fortsatta behandlingen ska således – utom i fall där andra punkten i denna paragraf blir tillämplig – alltid ske med stöd av bestämmelserna i 7 och 8 §§. Som exempel kan nämnas att den fortsatta behandlingen ska ske med stöd av 7 § 2, om det är fråga om personuppgifter som hör till en förundersökning.

Vidare får, enligt *punkten 2*, personuppgifter alltid behandlas om de har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Begreppet ”anmälan eller liknande” innefattar alla slag av framställningar till polisen. Oftast ryms framställ-

ningar av detta slag inom de i 7 § angivna ändamålen och ska då behandlas med stöd av den paragrafen, men i vissa fall kan innehållet i framställan vara sådant att behovskriteriet i 7 § inte är uppfyllt. Eftersom en framställan vanligtvis påfordrar något slag av handläggning hos myndigheten, har det ansetts nödvändigt med en särskild bestämmelse för personuppgiftsbehandling i dessa fall. 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 besvarandet av framställan.

Behandling av känsliga personuppgifter

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

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen. Uppgifter som avses i första stycket får också behandlas med stöd av 9 §.

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

Paragrafen anger i vilken utsträckning känsliga personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Frågan har behandlats i avsnitt 8.

Enligt *första stycket* får personuppgifter inte behandlas enbart på grund av vad som är känt om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Bestämmelsen överensstämmer i huvudsak med 5 § polisdatalagen (1998:622). Det är således inte tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån ras, etniskt ursprung eller något annat i paragrafen angivet kriterium kan hänföras till en viss kategori av människor.

En uppgift om utseende utgör normalt inte en sådan personuppgift som avses i första stycket och den får alltså behandlas, med den begränsning som följer av tredje stycket. Om en sådan uppgift samtidigt innefattar uppgift om ras eller etniskt ursprung, omfattas den dock av förbudet. Bestämmelsen i första stycket hindrar inte att uppgifter om en persons nationalitet behandlas, eftersom en sådan uppgift normalt inte ger upplysning om ras eller etniskt ursprung. Motsvarande bedömning har gjorts i förarbetena till lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (prop. 2001/02:144 s. 41). Uppgifter om att en viss person närmast kommer från en viss världsdel eller ett visst land faller också som regel utanför förbudet mot behandling av känsliga personuppgifter. Uppgifter om att N.N. är spansk medborgare, född i Spanien eller inrest från Spanien omfattas alltså inte av förbudet. Skulle emellertid en sådan uppgift i det enskilda fallet t.ex. avslöja etniskt ursprung faller den in under förbudet i första stycket.

Andra stycket innerhåller två undantag från huvudregeln, varav det ena motsvarar 5 § andra stycket polisdatalagen. För det första får uppgifter om en person som behandlas på annan grund kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen. Bestämmelsen innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får dessa kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung om det är av avgörande betydelse för utredningen. Under utredning av ett sexualbrott kan det t.ex. vara befogat att anteckna uppgifter om någon av de misstänktas sexualliv. Med hänsyn till den restriktivitet som ligger i begreppet ”absolut nödvändigt” måste dock behovet av att göra sådana kompletteringar prövas noga i det enskilda ärendet. Känsliga personuppgifter kan också förekomma i förundersökningar 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. Eftersom polisen inte kan hindra någon från att yttra sig vare sig muntligen eller skriftligen kan känsliga personuppgifter på detta sätt komma att ingå i 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 andra stycket.

För det andra får känsliga personuppgifter alltid behandlas i de fall som avses i 9 §, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i en anmälan eller liknande, om det är nödvändigt för handläggningen. Det innebär bl.a. att det är möjligt för polisen att ta emot och besvara anmälningar och liknande skrifter som lämnas i elektronisk form även om dessa innehåller känsliga personuppgifter. Som framgår av kommentaren till 9 § är den behandling som omfattas av bestämmelsen begränsad.

I *tredje 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. Exempel på signalementsbeteckningar som anses acceptabla finns bl.a. i Rikspolisstyrelsens föreskrifter och allmänna råd om fingeravtryck och fotografering (RPSFS 2000:16, FAP 473–1).

Som bestämmelserna i paragrafen har utformats är polisen alltid oförhindrad att, exempelvis 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. Anteckningarna måste dock – i enlighet med tredje stycket – utformas på ett objektivt sätt. I anslutning till dessa anteckningar får även sådana känsliga personuppgifter som avses i första stycket antecknas, under förutsättning att det är absolut nödvändigt för det polisarbete som tipset bör föranleda.

Tillgången till personuppgifter

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

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om tillgången till personuppgifter.

Paragrafen har behandlats i avsnitt 6.6.

I polisens brottsbekämpande verksamhet förekommer en betydande mängd uppgifter. Till stor del är dessa av integritetskänsligt slag och ska inte spridas till någon som inte är behörig att ta del av uppgifterna. I *första stycket* slås därför fast att tillgången till personuppgifter i polisens brottsbekämpande verksamhet alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen riktar sig inte bara till dem som är engagerade i polisens dagliga verksamhet. Den måste också beaktas av dem som ansvarar för utformningen av nya datasystem liksom av dem som avgör vilken tillgång till personuppgifter respektive tjänsteman behöver för att kunna fullgöra sina uppgifter.

I *andra stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela närmare föreskrifter om förutsättningarna för tillgången till personuppgifter. Detaljbestämmelser kan således utformas så att tillgången till personuppgifter begränsas till vad som är nödvändigt för verksamhetens bedrivande.

Bevarande och gallring

12 § Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de i lagen angivna ändamålen.

I följande bestämmelser anges hur länge uppgifter som behandlas automatiserat längst får bevaras:

1. 13 § om uppgifter som inte har gjorts gemensamt tillgängliga,
2. 3 kap. 9–13 §§ om uppgifter i ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga,
3. 3 kap. 14 och 15 §§ om andra uppgifter som har gjorts gemensamt tillgängliga än som anges i 2,
4. 4 kap. 7 § om uppgifter i register över DNA-profiler,
5. 4 kap. 14–16 §§ om uppgifter i fingeravtrycks- eller signalementsregister,
6. 4 kap. 20 § om uppgifter i penningtvättsregister, och
7. 4 kap. 22 § om uppgifter i det internationella registret.

Regeringen meddelar föreskrifter om digital arkivering.

Paragrafen innehåller en generell bestämmelse om längsta tid för bevarande av personuppgifter i den brottsbekämpande verksamheten och hänvisar till de övriga bestämmelser om bevarande och gallring som finns i lagen. Paragrafen, som har motiverats i avsnitt 14.1, omfattar all behandling enligt lagen förutom Säkerhetspolisens personuppgiftsbehandling. För sistnämnda behandling finns en motsvarande bestämmelse i 5 kap. 6 §.

Av *första stycket* följer att personuppgifter aldrig får bevaras under längre tid än vad som behövs för något eller några av lagens ändamål. De ändamål som avses är de som anges i 7–9 §§. Bevarande tillåts således med hänsyn till ett eller flera ändamål. Därigenom ges stöd för att bevara uppgifter, inte bara för ett visst utpekat konkret ärende som en viss förundersökning, utan även för mer övergripande brottsbekämpande ändamål. Bestämmelsen ger exempelvis stöd för att bevara uppgifter i ett

avslutat ärende, även om det vid tidpunkten då ärendet avslutas inte finns något konkret nytt ändamål för bevarandet men uppgifterna bedöms ha ett allmänt värde för polisens verksamhet att förebygga, förhindra och upptäcka brottslig verksamhet eller utreda och beivra brott. En grundläggande förutsättning för bevarandet är att polisen bedömer att uppgifterna behöver finnas tillgängliga ytterligare viss tid i den brottsbekämpande verksamheten för att polisen ska kunna fullgöra sin uppgift som brottsbekämpare. Första stycket avser såväl automatiserad som annan behandling av personuppgifter, t.ex. behandling i manuella register.

I *andra stycket* hänvisas till de övriga paragrafer i 2–4 kap. som innehåller bestämmelser om bevarande och gallring. Syftet med uppräkningen är att skapa en överblick av regleringen.

I *tredje stycket* informeras om att regeringen kan meddela föreskrifter om digital arkivering. Syftet med sådana föreskrifter kan vara att förhindra att digitalt arkiverade uppgifter fortsätter att behandlas på samma sätt som tidigare i den brottsbekämpande verksamheten, trots att bevarandet inte längre sker för verksamhetsändamål utan för arkivändamål.

13 § Personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga eller behandlas i särskilda register enligt 4 kap. ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Paragrafen reglerar gallring av personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga. Vad som avses med gallring har behandlats i avsnitt 14.1. Frågan om gallring av detta slag av uppgifter har behandlats i avsnitt 14.2.

Som framgår av *första stycket* ska personuppgifter som behandlas i ett ärende gallras senast ett år efter det att ärendet avslutades, medan personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången. Gallringsfristens längd beror alltså på om personuppgifterna behandlas inom ramen för ett ärende eller inte. Begreppet ärende har här en särskild innebörd som kan avvika från den innebörd som begreppet har i förvaltningslagen (1986:223). Med ärende avses en serie åtgärder som är avsedda att leda fram till ett bestämt slut. Särskilda underrättelseprojekt kan t.ex. omfattas. Underrättelseprojekt med en obestämd varaktighet, exempelvis ett projekt som syftar till att fortlöpande undersöka ungdomsbrottsligheten på en viss ort, kan dock inte anses som ett ärende i den mening som avses i paragrafen. Åtgärder som vidtas med anledning av att någon enskild har påkallat att polisen agerar får anses som ett ärende. Det är däremot inte fråga om något ärende när en polisman vidtar en tillfällig åtgärd inom ramen för polisens allmänna brottsförebyggande verksamhet, t.ex. tar emot ett tips från allmänheten som inte har samband med en pågående brottsutredning eller ett underrättelseprojekt. Bestämmelsen är

inte tillämplig på uppgifter som har gjorts gemensamt tillgängliga eller som behandlas i särskilda register med stöd av 4 kap. För sådana uppgifter gäller särskilda gallringsregler i 3 kap. 14 och 15 §§ respektive i 4 kap 7, 14–16, 20 och 22 §§.

I andra och tredje styckena föreskrivs två undantag från gallringsbestämmelserna i första stycket. Enligt *andra stycket* gäller inte gallringsbestämmelserna personuppgifter i ärenden om utredning eller beivrande av brott. Det rör sig framförallt om förundersökningar och om andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken (se kommentaren till 7 §). I fråga om uppgifter i sådana ärenden tillämpas i stället bestämmelserna om gallring i arkivlagen (1990:782).

Av *tredje stycket* följer att regeringen eller den myndighet regeringen bestämmer har möjlighet att meddela föreskrifter om att personuppgifter, trots vad som sägs i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utlämnande av personuppgifter och uppgiftsskyldighet

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

Enligt paragrafen, som motsvarar 6 § polisdatalagen (1998:622), ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för framställandet av sådan statistik. Bestämmelsen, vars bakgrund har beskrivits i avsnitt 13.2, bryter den sekretess som kan gälla för personuppgifterna.

Av förordningen (2001:100) om den officiella statistiken framgår att Brottsförebyggande rådet är statistikansvarig myndighet på rättsväsendets område, med undantag för domstolarnas verksamhet.

15 § Om det är förenligt med svenska intressen, får personuppgifter lämnas till

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

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

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande till utländska myndigheter och mellanfolkliga organisationer. Frågan har behandlats i avsnitt 13.3.

Inom ramen för de allmänna ändamålen för personuppgiftsbehandling i 7 § 1 och 2 kan det i vissa fall finnas anledning att föra över uppgifter till en utländsk myndighet. Ett exempel är när en svensk myndighet i en svensk brottsutredning begär rättsligt bistånd från en utländsk myndighet eller när en svensk myndighet aktualiserar en fråga om överförande av lagföring till utlandet. Av 7 § 3 framgår att personuppgifter får behandlas för att fullgöra de förpliktelser som följer av internationella åtaganden (se kommentaren till den paragrafen angående innebörden). Även i sådana

fall blir det ofta aktuellt att lämna information till en utländsk myndighet. Det kan t.ex. vara fråga om att en utländsk myndighet med stöd av en internationell överenskommelse begär utlämning, överlämnande enligt den europeiska arresteringsordern eller rättslig hjälp. I sådana fall måste personuppgifter behandlas bl.a. för att konstatera om personen finns i Sverige. Vidare innehåller 8 § en bestämmelse om att personuppgifter som behandlas enligt 7 § också får behandlas för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation. De nu angivna bestämmelserna sätter gränserna för när behandling som har till ändamål att överföra information till en utländsk myndighet eller organisation över huvud taget får förekomma.

För att sådant utlämnande ska få ske krävs därutöver att det inte på grund av sekretess finns hinder mot att lämna över uppgifterna till den utländska mottagaren. För många av de personuppgifter som förekommer hos polisen gäller sekretess, såväl till skydd för intresset av att förebygga och beivra brott som till skydd för enskilds ekonomiska eller personliga förhållanden. Enligt 8 kap. 3 § offentlighets- och sekretesslagen (2009:400) får en sekretessbelagd uppgift inte röjas för en utländsk myndighet eller en mellanfolklig organisation annat än om utlämnandet sker i enlighet med en särskild föreskrift om detta i lag eller förordning eller om uppgiften i motsvarande fall skulle få utlämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen. I vissa fall kan en utlämnandeprövning enligt nämnda paragraf vara komplicerad. I paragrafen anges därför vissa mera preciserade fall där uppgifter får lämnas ut till en utländsk mottagare, trots att det gäller sekretess för uppgiften. Bestämmelsen i paragrafens första stycke överensstämmer i huvudsak med 18 § polisdataförordningen (1999:81). Bestämmelsen i paragrafens andra stycke överensstämmer i huvudsak med 7 § första stycket polisdatalagen (1998:622).

Enligt *första stycket* får uppgifter, om det är förenligt med svenska intressen, lämnas till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, till Interpol och Europol (*punkten 1*) samt till utländsk underrättelse- eller säkerhetstjänst (*punkten 2*). Utlämnande av uppgifter till polis- eller åklagarmyndigheter, samt till Interpol eller Europol, får ske endast om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott. Bestämmelsen ger utrymme för svenska myndigheter att lämna ut uppgifter såväl på begäran som utan föregående framställning.

I *andra stycket* föreskrivs att personuppgifter får lämnas ut till en utländsk myndighet eller en mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Bestämmelsen är tillämplig när den internationella överenskommelsen ålägger Sverige att lämna ut vissa slag av uppgifter. Däremot gäller den inte för överenskommelser där det enbart sägs att utlämnande *får* ske. I sådana fall kan bestämmelserna i första stycket vara tillämpliga eller också kan en prövning göras enligt 8 kap. 3 § offentlighets- och sekretesslagen.

Oavsett vilken bestämmelse som tillämpas som stöd för utlämnandet, måste, som utvecklas närmare i avsnitt 13.3, den utlämnande myndigheten försäkra sig om att den mottagande staten har en adekvat nivå för skydd av personuppgifter innan några uppgifter lämnas ut (se 2 § första stycket 8).

16 § Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Första stycket gäller inte uppgifter som behandlas i särskilda register enligt 4 kap.

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Frågan har behandlats i avsnitt 13.2.

I *första stycket* regleras brottsbekämpande myndigheters rätt att, trots viss i paragrafen angiven sekretess till skydd för enskild, i den brottsbekämpande verksamheten få del av personuppgifter som har gjorts gemensamt tillgängliga inom polisen. Eftersom sekretess kan hindra att uppgifter lämnas ut, har undantag gjorts för vissa typer av sekretess, där sekretessen är lika stark hos den mottagande myndigheten som hos den utlämnande. Paragrafen har utformats som en uppgiftsskyldighet (jfr prop. 2007/08:160 s. 54). En förutsättning för att uppgifter ska lämnas ut är dock att det finns ett behov av uppgifterna i den brottsbekämpande verksamheten hos den mottagande myndigheten. Det är den utlämnande myndigheten som ytterst avgör om den andra myndigheten behöver uppgifterna.

Med polismyndighet avses även Säkerhetspolisen när den för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet (se 7 § andra stycket polislagen [1984:387] jämförd med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen). När Säkerhetspolisen utför andra uppgifter (3 § samma förordning) är den en del av Rikspolisstyrelsen. Uppgifter som behandlas hos den övriga polisen kan således utan hinder av i paragrafen angiven sekretess lämnas till Säkerhetspolisen.

I *andra stycket* görs undantag för uppgifter som behandlas i de register som regleras särskilt i 4 kap. Om sådana uppgifter kan lämnas ut får, som huvudregel, avgöras efter en sekretessbedömning i det enskilda fallet. Som framgår av 17 och 18 §§ gäller dock särskilda bestämmelser om utlämnande av uppgifter i register över DNA-profiler och fingeravtrycks- eller signalementsregister.

17 § Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av uppgifter om huruvida personer förekommer i register över DNA-profiler, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Uppgifter ur sådana register ska lämnas till Statens kriminaltekniska laboratorium, om myndigheten behöver uppgifterna i sin verksamhet.

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Frågan har behandlats i avsnitt 13.2.

I paragrafens *första stycke* anges vilka myndigheter som har rätt att, trots sekretess till skydd för enskild enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), i den brottsbekämpande verksamheten få del av uppgifter ur register över DNA-profiler, dvs. DNA-registret, utredningsregistret och spårregistret. Endast uppgifter om huruvida personer förekommer i sådana register får lämnas ut. En förutsättning för att uppgifterna ska få lämnas ut är att de behövs för den brottsbekämpande verksamheten hos den mottagande myndigheten. Vad som sägs i kommentaren till 16 § angående behovet av uppgifter gäller även här.

I *andra stycket* föreskrivs att Statens kriminaltekniska laboratorium ska, utan hinder av sekretess, få del av uppgifter ur register över DNA-profiler. Eftersom laboratoriet i sin verksamhet hanterar alla uppgifter som förekommer i de olika registren har den myndigheten, till skillnad från de myndigheter som anges i första stycket, rätt att få del av samtliga uppgifter i de aktuella registren.

De myndigheter som har rätt att få del av vissa uppgifter med stöd av paragrafen är desamma som de som med stöd av 4 kap. 10 § kan medges direktåtkomst till register över DNA-profiler. Vad som sägs i kommentaren till 16 § om Säkerhetspolisens tillgång till uppgifter gäller även här.

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som behandlas i fingeravtrycks- eller signalementsregister enligt 4 kap. 11–17 §§, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Detsamma gäller Statens kriminaltekniska laboratorium, om myndigheten behöver uppgifterna i sin verksamhet.

Paragrafen, som har behandlats närmare i avsnitt 13.2, innehåller, liksom 16 och 17 §§, en sekretessbrytande bestämmelse. Enligt *första meningen* kan uppgifter ur fingeravtrycks- eller signalementsregister lämnas ut till de där angivna myndigheterna trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400). För att uppgifter ska få lämnas ut krävs att de behövs för den brottsbekämpande verksamheten hos den mottagande myndigheten. Vad som sägs i kommentaren till 16 § angående behovet av uppgifterna gäller även här. I *andra meningen* föreskrivs att också Statens kriminaltekniska laboratorium har motsvarande rätt att få del av uppgifter som behandlas i fingeravtrycks- eller signalementsregister. En förutsättning är att uppgifterna behövs i laboratoriets verksamhet.

Den krets av myndigheter som har rätt att få del av personuppgifter som behandlas i fingeravtrycks- eller signalementsregister motsvarar de myndigheter som enligt 4 kap. 17 § får medges direktåtkomst till registren i fråga. Vad som sägs i kommentaren till 16 § om Säkerhetspolisens tillgång till uppgifter gäller även här.

19 § Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 14–18 §§.

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

Paragrafen har motiverats i avsnitt 13.2 och 13.3.

I *första stycket* finns en upplysning om att regeringen har möjlighet att meddela föreskrifter om att personuppgifter får lämnas ut även i andra fall än som anges i 14–18 §§. Det kan t.ex. vara aktuellt med föreskrifter som motsvarar 17 § polisdataförordningen (1999:81), som medger utlämnande av uppgifter om bl.a. avlägsnanden ur landet. Vidare kan det behövas föreskrifter som möjliggör för Finanspolisen att lämna ut uppgifter till utländska myndigheter som har motsvarande uppdrag att ta emot och lämna ut information om misstänkt penningtvätt eller finansiering av terrorism (se kommentaren till 4 kap. 19 §). Det kan nämligen förekomma att en utländsk myndighet som bekämpar sådan brottslighet inte ingår i den statens polis- eller åklagarväsende. Möjligheten att lämna ut uppgifter omfattas därmed inte av 15 § första stycket 1.

I *andra stycket* erinras om att det i offentlighets- och sekretesslagen (2009:400) finns bestämmelser om utlämnande som gäller utöver vad som anges i lagen. Utlämnande kan exempelvis ske med stöd av generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen. En annan sådan bestämmelse, som rör utlämnande till utländska myndigheter eller mellanfolkliga organisationer, finns i 8 kap. 3 § offentlighets- och sekretesslagen.

Elektroniskt utlämnande av personuppgifter

20 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen meddelar föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall.

Paragrafen reglerar utlämnande av uppgifter på medium för automatiserad behandling, medan direktåtkomst regleras i 21 §. I paragrafen anges under vilka förutsättningar uppgifter får lämnas ut t.ex. i ett e-postmeddelande eller på ett USB-minne. Frågan har behandlats i avsnitt 12.1 och 12.4.

Bestämmelsen, som inte har någon sekretessbrytande verkan, innebär att en större mängd personuppgifter, t.ex. ett helt register eller delar av ett register, inte får lämnas ut på medium för automatiserad behandling, såvida inte regeringen har meddelat föreskrifter om detta. Däremot kan, enligt *första meningen*, enstaka uppgifter lämnas ut. Uttrycket enstaka används här med en något annan innebörd än i vanligt språkbruk. När personuppgifter förekommer i en eller ett fåtal handlingar är bestämmelsen inte avsedd att utgöra ett hinder mot att handlingarna lämnas ut genom t.ex. ett e-postmeddelande. Det förhållandet att en handling, t.ex. en lista över telefonnummer, innehåller ett större antal personuppgifter hindrar inte att handlingen lämnas ut med stöd av paragrafen. Bestämmelsen är också avsedd att ge stöd för utlämnande av t.ex. ett ärende eller delar av ett ärende där personuppgifter förekommer (jfr prop. 2006/07:46 s. 124). Av *andra meningen* följer att regeringen har möjlighet att med-

dela föreskrifter om utlämnande av större uppgiftsmängder, t.ex. mellan myndigheter.

21 § Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag.

Regeringen meddelar föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, om detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 § samt 4 kap. 10 och 17 §§.

Paragrafen reglerar direktåtkomst. Frågor om direktåtkomst har behandlats i avsnitt 12.1–12.3. Den grundläggande innebörden av begreppet direktåtkomst är att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I begreppet direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av. Om någon har direktåtkomst till samtliga uppgifter i en myndighets register, kan denne alltså själv välja vilka uppgifter han eller hon vill ta del av vid ett visst tillfälle, utan att myndigheten först fattar ett beslut om att just dessa uppgifter ska lämnas ut. Bestämmelserna om direktåtkomst har inte någon sekretessbrytande verkan.

I *första stycket* görs klart att direktåtkomst bara får förekomma i den utsträckning som följer av denna lag. Det innebär bl.a. att det ska framgå av lagen om och i vilken utsträckning bestämmelser om direktåtkomst får meddelas på lägre normgivningsnivå.

I *andra stycket* informeras om att regeringen har möjlighet att meddela föreskrifter om att utländska myndigheter, Europol och mellanfolkliga organisationer får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet i den utsträckning detta följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Det finns sådana åtaganden i Prümrådsbeslutet (avsnitt 4.4.3). Detsamma gäller om åtagandet följer av en bindande EU-rättsakt. Frågan om direktåtkomst för utländska myndigheter har behandlats i avsnitt 12.3.5.

I *tredje stycket* anges vilka övriga bestämmelser i lagen som reglerar direktåtkomst. Syftet är att skapa en överblick över regleringen.

3 kap. Gemensamt tillgängliga uppgifter

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

Bestämmelserna i detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 9 §.

Som närmare utvecklats i avsnitt 9.1 bygger den föreslagna lagen på en uppdelning mellan å ena sidan behandling av ”gemensamt tillgängliga uppgifter” eller behandling som innebär att uppgifter blir gemensamt tillgängliga och å andra sidan annan behandling av personuppgifter. I paragrafens *första stycke* anges att bestämmelserna i 3 kap. gäller vid behandling av det förra slaget.

Avgörande för bedömningen av om personuppgifter är att anse som gemensamt tillgängliga eller inte är om uppgifterna är åtkomliga för en bestämd och begränsad personkrets. Om avsikten är att uppgifterna ska vara åtkomliga för en i förväg obestämd krets av anställda inom polisen, får uppgifterna alltid anses vara gemensamt tillgängliga. Som exempel på detta kan nämnas uppgifter i polisens nationella uppgiftssamlingar men även lokala register där det inte på förhand har bestämts vilka personer som får ha tillgång till uppgifterna. Att olika personalkategorier kan ha olika behörighet, och att en uppgift därför i praktiken vid en viss tidpunkt är åtkomlig enbart för ett begränsat antal personer, innebär alltså inte att uppgiften inte kan anses vara gemensamt tillgänglig. Uppgifter som en annan brottsbekämpande myndighet har tillgång till genom direktåtkomst är alltid gemensamt tillgängliga, se kommentaren till 3 kap. 8 §.

Om uppgifterna å andra sidan lagras på ett sådant sätt att endast en viss person har tillgång till dem, kan uppgifterna normalt inte anses gemensamt tillgängliga. Personuppgifter som lagras elektroniskt på hårddisken i en dator eller en server i samband med att en enskild tjänsteman arbetar med ordbehandling och som är åtkomliga endast för tjänstemannen själv (och för systemadministratören) kan alltså inte anses vara gemensamt tillgängliga. Detsamma gäller digitala upptagningar av bild eller ljud, om endast den som samlar in uppgifterna har tillgång till dessa. I sådana fall är bestämmelserna i 3 kap. inte tillämpliga. Detta gäller även om syftet är att uppgifterna senare ska lagras så att andra får tillgång till dem. Det är alltså först när insamlade uppgifter görs tillgängliga för fler än ett fåtal personer i den brottsbekämpande verksamheten som bestämmelserna i 3 kap. ska tillämpas. En annan sak är att den som samlar in uppgifter, som kan antas bli gemensamt tillgängliga vid en senare tidpunkt, redan vid insamlingstillfället bör beakta de särskilda regler som gäller för behandling av gemensamt tillgängliga personuppgifter för att inte försvåra den fortsatta behandlingen.

I vad mån uppgifter som är tillgängliga enbart för en bestämd krets av personer är att anse som gemensamt tillgängliga får bedömas med hänsyn till främst hur många personer som har tillgång till uppgifterna. Enbart det förhållandet att fler än en har tillgång till uppgifterna innebär inte att uppgifterna ska anses gemensamt tillgängliga. Behandlingar som sker exempelvis inom ramen för särskilda underrättelseprojekt i vilka endast vissa utpekade tjänstemän deltar, kan alltså falla utanför regleringen i 3 kap. Om antalet tjänstemän i en sådan grupp uppgår till fler än ett fåtal, måste dock de personuppgifter som behandlas inom gruppen, trots att den är avgränsad, anses vara gemensamt tillgängliga. Var gränsen går får bedömas med hänsyn till samtliga omständigheter i ett enskilt fall, men en tumregel kan vara att uppgifterna är att anse som gemensamt tillgängliga om antalet deltagare i gruppen överstiger ett tiotal.

Även den tid under vilken uppgifter avses bli behandlade kan ha betydelse för frågan om uppgifterna ska anses vara gemensamt tillgängliga

eller inte. I projekt med längre varaktighet måste man räkna med att de personer som sysslar med projektet med tiden kommer att bytas ut. Som en följd av detta kommer de uppgifter som behandlas att bli tillgängliga för ett större antal personer än vad som motsvarar det normala antalet deltagare i projektet. Mot den bakgrunden kan uppgifter som behandlas i långsiktiga projekt ibland anses vara gemensamt tillgängliga, trots att antalet deltagare vid varje givet tillfälle är begränsat till en mindre grupp av personer.

När det gäller frågan om huruvida en uppgift är gemensamt tillgänglig eller inte är det viktigt att framhålla att karaktären av en uppgift kan förändras under den tid som den behandlas. Uppgifter som från början har betraktats som icke gemensamt tillgängliga kan göras gemensamt tillgängliga. Det kan t.ex. bli nödvändigt att göra viss underrättelseinformation tillgänglig för tjänstemän utanför det aktuella underrättelseprojektet. När så har skett ska de strängare bestämmelserna om behandling av gemensamt tillgängliga uppgifter tillämpas.

Som exempel på existerande uppgiftssamlingar där uppgifterna måste anses gemensamt tillgängliga kan nämnas det centrala kriminalunderrättelseregistret, det centrala brottsspaningsregistret och beslags- och analysregistren. Som nyss nämnts bör även uppgifter i större särskilda undersökningar anses vara gemensamt tillgängliga.

Av *andra stycket* följer att bestämmelserna i 3 kap. inte gäller när personuppgifter behandlas med stöd av bestämmelserna i 2 kap. 9 § om diarieföring m.m. I kommentaren till den paragrafen utvecklas närmare vilken personuppgiftsbehandling som får ske med stöd av denna.

Personuppgifter som får göras gemensamt tillgängliga

2 § Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, om han eller hon

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra vad som följer av internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.

5. Uppgifter som har rapporterats till polisens kommunikationscentraler.

DNA-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

När personuppgifter görs gemensamt tillgängliga innebär det, typiskt sett, ökade risker för intrång i den personliga integriteten. Paragrafens

första stycke innehåller därför en uppräkning av de slag av personuppgifter som får göras gemensamt tillgängliga. Uppräkningen är uttömmande och det är alltså inte tillåtet att göra personuppgifter gemensamt tillgängliga i andra fall.

I *punkten 1*, som har behandlats närmare i avsnitt 9.2, nämns personuppgifter ”som kan antas ha samband med misstänkt brottslig verksamhet”. Rekvisitet innebär att det måste finnas en misstanke om att sådan brottslig verksamhet som avses 2 kap. 7 § 1 har utövats eller kommer att utövas. Den brottsliga verksamheten måste vara på visst sätt kvalificerad. Huvudregeln är att den ska innefatta brott för vilket det är föreskrivet fängelse i ett år eller däröver. Detta innebär att alla brott som enligt huvudregeln i 24 kap. 1 § rättegångsbalken kan föranleda häktning omfattas. Även om den brottsliga verksamheten inte innefattar brott med en sådan straffskala får personuppgifter som kan antas ha samband med den brottsliga verksamheten göras gemensamt tillgängliga, om det kan antas att verksamheten sker systematiskt. Ett exempel kan vara om verksamheten innefattar enbart bedrägligt beteende i form av s.k. snyltning, dvs. att inte göra rätt för sig på hotell och liknande. Med ”verksamhet som sker systematiskt” avses detsamma som i 12 § första stycket 1 a lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. I förarbetena till den bestämmelsen nämns bl.a. som exempel en person som för in en mindre mängd cigaretter för privat bruk. Personen i fråga gör dock så frekventa resor att den totala mängden infört gods ger anledning att anta att det inte är för privat bruk utan för återförsäljning, s.k. myrtrafik (prop. 2004/05:164 s. 71 f.). Ett liknande exempel ges i fråga om kurirer som smugglar små mängder narkotika.

Att personuppgifterna ”kan antas ha samband” med den brottsliga verksamheten innebär att de ska kunna antas ha någon direkt eller indirekt koppling till den brottsliga verksamheten.

Det kan vara fråga om uppgifter om en misstänkt, en målsägande, ett vittne eller någon annan person som har en anknytning till brottsligheten. En affärspartner till den misstänkte kan ibland ha en sådan anknytning, exempelvis om man misstänker att den brottsliga verksamheten helt eller delvis bedrivs i samma lokal som affärsverksamheten. På samma sätt kan en anhörig till en misstänkt ha en sådan anknytning, t.ex. om den misstänkte regelmässigt uppehåller sig hos personen i fråga under den tid som den brottsliga verksamheten misstänks bedrivas. Det kan också vara fråga om indirekta personuppgifter, t.ex. adressuppgifter eller uppgifter om transportmedel eller andra föremål.

Det följer av 2 kap. 7 § 1 att uppgifterna alltid ska behövas i arbetet med att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Punkten 2, som har behandlats närmare i avsnitt 9.2, avser personuppgifter som behövs för övervakningen av vissa personer som kan antas komma att begå brott med två års fängelse eller däröver i straffskalan. Bestämmelsen anknyter till den särskilda bevakning av grovt kriminella som polisen redan bedriver. Den torde få sin främsta betydelse ifråga om personer som bedöms mer eller mindre livnära sig på allvarlig brottslig verksamhet, t.ex. organiserad brottslighet i form av grov narkotikasmuggling eller människohandel. Bedömningen av om en person kan antas komma att begå brott får i första hand göras på grund av tidigare domar. Även pågående brottsutredningar och underrättelseuppgifter kan

beaktas. Enbart det faktum att en person kan antas vara brottsbenägen räcker dock inte för att uppgifter om honom eller henne ska få göras gemensamt tillgängliga. Därutöver krävs endera av två saker. Den ena är att personens tidigare brottslighet är av allvarligt slag – varvid ett riktmärke kan vara att den bedömts ha ett straffvärde på minst två års fängelse. Den andra är att personen kan antas utgöra ett hot mot andras personliga säkerhet. Med det avses att han eller hon, oberoende av om vederbörande är straffad för allvarlig brottslighet eller inte, utgör ett latent hot mot andras liv, hälsa, frihet eller frid. Personen kan t.ex. genom sitt samröre med mycket våldsbenägna personer injaga fruktan i andra eller ha sådan tillgång till vapen som i sig kan uppfattas som hotfull.

Med stöd av punkten 2 får också mera allmänna uppgifter om den övervakade personen göras gemensamt tillgängliga. Det behöver alltså inte – till skillnad från vad som gäller enligt punkten 1 – finnas något antaget samband mellan personuppgiften och viss brottslig verksamhet. Det finns därför ett större utrymme att behandla uppgifter om anhöriga, bekanta m.fl. enligt denna punkt. Uppgifterna måste dock alltid vara relevanta för övervakningen och – som följer av 2 kap. 7 § 1 – nödvändiga för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Av *punkten 3*, som har behandlats närmare i avsnitt 9.3, framgår att personuppgifter som ingår i ett ärende om utredning eller beivrande av brott alltid får göras gemensamt tillgängliga. Det handlar här om personuppgifter som behandlas med stöd av 2 kap. 7 § 2.

Punkten 4, som har behandlats i avsnitt 9.5, innebär att det är tillåtet att göra sådana uppgifter gemensamt tillgängliga som behövs för att fullgöra internationella åtaganden, under förutsättning att det krävs att uppgifterna görs gemensamt tillgängliga för att fullgöra detta. Om utländska uppgifter föranleder en svensk brottsutredning eller ett svenskt underrättelseprojekt, behandlas uppgifterna med stöd av de primära ändamålen i 2 kap. 7 § 1 eller 2 och kan då göras gemensamt tillgängliga på samma sätt som andra uppgifter som förekommer i ett sådant ärende. De personuppgifter som får göras gemensamt tillgängliga enligt punkten 4 är bl.a. sådana internationella efterlysningar av personer eller föremål som kommer från andra länder. Dessa uppgifter är avsedda att spridas inom polisorganisationen. När brottsbekämpande myndigheter i Sverige bedriver brottsutredningar tillsammans med sina motsvarigheter i andra länder eller när man i flera länder bedriver parallella brottsutredningar eller samlar underrättelseinformation om samma brottslighet (exempelvis narkotikabrottslighet eller människohandel), kan det också finnas ett behov av att göra uppgifterna gemensamt tillgängliga. Det internationella samarbetet bygger i allt större utsträckning på att länderna har nationella kontaktpunkter för vissa typer av brådskande ärenden. En sådan kontaktpunkt ska vara tillgänglig dygnet runt året om för att besvara förfrågningar, förmedla kontakter till polis och åklagare, vidarebefordra ärenden m.m. De uppgifter som lämnas till en nationell kontaktpunkt måste av bl.a. praktiska skäl vara gemensamt tillgängliga för att åtagandena ska kunna fullgöras.

Uppgifterna får göras gemensamt tillgängliga enbart i den utsträckning det krävs för att fullgöra den internationella förpliktelsen. Det finns situationer där uppgifter behandlas inom ramen för internationellt samarbete utan att det finns något behov av att göra uppgifterna gemensamt

tillgängliga. Så kan t.ex. vara fallet vid rättslig hjälp, då det ofta förekommer direktkommunikation mellan myndigheterna i olika länder. I fall där den rättsliga hjälpen rör en viss bestämd fråga i ett enskilt ärende, torde det normalt inte finnas något behov av att göra de behandlade personuppgifterna gemensamt tillgängliga.

Enligt *punkten 5* får även uppgifter som har rapporterats till polisens kommunikationscentraler göras gemensamt tillgängliga. Motiven för denna bestämmelse har redovisats i avsnitt 9.4. Eftersom lagen enbart gäller för den brottsbekämpande verksamheten hos polisen, är det bara rapporter som har relevans för sådan verksamhet, dvs. som omfattas av 2 kap. 7 §, som får göras gemensamt tillgängliga med stöd av denna punkt. För övrig verksamhet vid kommunikationscentralerna tillämpas personuppgiftslagen (1998:204), se avsnitt 6.3.

Enligt *andra stycket*, som har behandlats närmare i avsnitt 9.6, får DNA-profiler inte göras gemensamt tillgängliga. Däremot får sådana uppgifter behandlas i vissa särskilda register enligt 4 kap., om förutsättningarna i övrigt för en sådan behandling är uppfyllda. Vad som avses med en DNA-profil behandlas i kommentaren till 2 kap. 3 §. Bestämmelsen hindrar inte att exempelvis utlåtanden över DNA-profiler behandlas utan tar endast sikte på behandlingen av DNA-profilen som sådan.

I *tredje stycket* kompletteras den allmänna bestämmelsen i 2 kap. 11 § med en bestämmelse som särskilt begränsar tillgången till uppgifter som behandlas för att underlätta övervakningen av grovt kriminella personer enligt första stycket punkten 2. Endast de tjänstemän som arbetar med denna övervakning får ha tillgång till uppgifterna. Tillgången till uppgifter behöver däremot inte begränsas till tjänstemän vid en viss myndighet. Vid varje myndighet ska det dock i förväg bestämmas vilka tjänstemän som ska ha tillgång till uppgifterna och ha möjlighet att behandla dem, bl.a. i analysdatabaser. I andra meningen görs ett undantag från begränsningsregeln. Information om att en person är övervakad med stöd av aktuell bestämmelse får spridas till andra. Även här gäller dock den allmänna begränsningen att mottagaren måste ha behov av uppgiften för sitt arbete.

Särskilda upplysningar

3 § Vid behandling enligt 1 § ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska detta särskilt framgå.

I paragrafen uppställs krav på att de närmare ändamålen med behandlingen ska framgå. Skälen till regleringen har utvecklats i avsnitt 10.

Enligt *första meningen* ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Det ska vara tydligt för vilket slag av brott eller brottslig verksamhet etc. som behandlingen sker, exempelvis ett underrättelseprojekt om vapensmuggling från Y-land.

I *andra meningen* föreskrivs att om uppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, så ska detta särskilt framgå. Det ska således framgå om en personuppgift har gjorts gemen-

samt tillgänglig som ett led i övervakningen av en allvarligt kriminellt belastad person. Vidare ska det framgå om en uppgift behandlas för att den har rapporterats till en kommunikationscentral.

De aktuella förhållandena ska framgå genom en särskild upplysning eller på något annat sätt. Detta innebär att en särskild upplysning endast behövs i de fall där förhållandet inte redan framgår av omständigheterna. Ofta framgår det av omständigheterna för vilket närmare ändamål behandlingen sker. En personuppgift som t.ex. behandlas i ett register över övervakade grovt kriminella personer (2 § första stycket 2) behöver därför vanligen inte kompletteras med någon särskild upplysning, vare sig enligt första eller andra meningen. Om uppgiften förekommer i en förundersökning behövs det inte heller någon särskild upplysning, eftersom varje förundersökning ska röra visst eller vissa angivna brott. På motsvarande sätt behövs det normalt inte någon särskild upplysning beträffande uppgifter som behandlas i ett avgränsat underrättelseprojekt, t.ex. en särskild undersökning, om detta har ett tydligt definierat ändamål.

Vid behandling av uppgifter i bild- eller ljudupptagningar eller i löpande text framgår det också i regel klart av sammanhanget varför uppgifterna behandlas. Varje enskild uppgift måste således inte förses med en särskild upplysning, vilket inte heller torde vara praktiskt möjligt. Upptagningen, textfilen eller textavsnittet ska dock förses med en särskild upplysning om ändamålet, om detta inte framgår på något annat sätt. Det är av skäl som nyss angetts som regel tillräckligt att det framgår att upptagningen härrör t.ex. från en viss angiven förundersökning.

Om en uppgift har samlats in för visst ändamål och senare kommer att användas för något nytt ändamål, måste det vid den senare behandlingen framgå att behandlingen sker för ett nytt ändamål. Om uppgifter från en förundersökning avseende visst brott senare används i kriminalunderrättelseverksamhet avseende annan brottslighet, måste det nya ändamålet således framgå.

4 § Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, 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 samband med misstänkt brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte detta på grund av särskilda omständigheter är onödigt. Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.

I paragrafen ställs krav på att det vid behandling av uppgifter som har gjorts gemensamt tillgängliga ska framgå om en uppgift avser en person som inte är misstänkt. Vidare ställs krav på att viss information ska värderas och förses med en särskild upplysning om resultatet av värderingen. Frågan har behandlats i avsnitt 10.

Bestämmelserna avser endast direkta personuppgifter. Om den person som uppgiften avser inte är misstänkt vare sig för något brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, följer av *första stycket* att detta förhållande ska framgå genom en särskild upplysning eller på något annat sätt. Kravet gäller endast om det inte finns några som helst misstankar mot den aktuella

personen. Förekommer det någon form av misstanke – vare sig det handlar om ”skälig misstanke” eller om någon annan misstankegrad – behöver någon tilläggsupplysning inte lämnas.

Om det framgår av sammanhanget att det inte är fråga om en misstänkt person behöver någon särskild upplysning inte lämnas. Om en person har hörts under en förundersökning men det av sammanhanget framgår att han eller hon har hörts endast som målsägande eller vittne, behöver således uppgifterna inte förses med någon tilläggsupplysning. Kravet på att det ska framgå om en person inte är misstänkt innebär att det krävs rutiner för att följa upp om en tidigare brottsmisstanke avskrivs i sin helhet, exempelvis i samband med att en förundersökning läggs ned, eller om rätten meddelar frikännande dom.

Vid behandling av uppgifter i bild- eller ljudupptagningar eller i löpande text framgår det som regel av sammanhanget om uppgiften rör en misstänkt eller inte. Varje enskild uppgift måste således inte förses med en särskild upplysning, vilket inte heller torde vara praktiskt möjligt. Det kan t.ex. röra sig om bilder från en viss plats, där syftet med bilden enbart är att illustrera de geografiska förhållandena men där personer syns på bilderna. Ibland kan dock upptagningen, textfilen eller textavsnittet behöva förses med en särskild upplysning som förtydligar att vissa personer, exempelvis personer som förekommer i en bildupptagning, inte är misstänkta. Om det finns flera personer på en bild och det av sammanhanget framgår att en av dessa är misstänkt framgår motsatsvis att de övriga inte är misstänkta.

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet eller som övervakas enligt 2 § första stycket 2 förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Kravet gäller endast för uppgifter som behandlas utan att det finns misstanke om något konkret brott, dvs. uppgifter som behandlas för ändamålet förebygga, förhindra eller upptäcka brottslig verksamhet. Bestämmelsen är således inte tillämplig på uppgifter som behandlas i brottsutredande verksamhet.

Upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak behöver inte lämnas om detta på grund av särskilda omständigheter skulle vara onödigt. Så kan exempelvis vara fallet om uppgifter om en viss person hämtas från offentliga register, t.ex. adress- och telefonuppgifter. Framgår det att en uppgift har lämnats av en polisman krävs det normalt inte någon värdering av eller upplysning om trovärdigheten. Däremot ska en bedömning av riktigheten i sak alltid göras, eftersom en iakttagelse eller bedömning kan vara osäker oberoende av vem som gör den.

Sökning

5 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Det som anges i första stycket hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Paragrafen reglerar användningen av känsliga personuppgifter som sökbegrepp. Frågan har behandlats i avsnitt 11.2. I avsnitt 8 och i kommentaren till 2 kap. 10 § redogörs närmare för vad som avses med känsliga personuppgifter.

I *första stycket* föreskrivs ett förbud mot att använda känsliga personuppgifter (dvs. uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv) som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter.

I *andra stycket* klargörs att förbudet inte hindrar att polisen använder brottsrubriceringar som sökbegrepp. Uppgifter som beskriver en persons utseende, t.ex. uppgifter om längd, hudfärg eller tatueringar, får också användas som sökbegrepp, även om sådana uppgifter kan ge indikationer om personens etniska ursprung.

6 § Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1,
4. övervakas enligt 2 § första stycket 2,
5. har anmält ett brott,
6. är målsägande i ett ärende som rör ansvar för brott,
7. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,
8. har gett in eller tillhandahållits en handling,
9. är anmäld såsom försvunnen,
10. har bedömts kunna komma att möta ett polisingripande med grovt våld, eller
11. är efterlyst.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om begränsning av tillgången till sådana uppgifter som avses i första stycket.

Paragrafen innehåller en allmän sökbegränsning vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer eller liknande identitetsbeteckningar. Frågan har behandlats i avsnitt 11.3.

Mot bakgrund av att de informationsmängder som kan göras gemensamt tillgängliga i polisens brottsbekämpande verksamhet sammantaget kan bli betydande är det av integritetsskäl inte lämpligt att tillåta fri sökning i informationen. Visserligen kan namn och andra liknande identitetsbeteckningar alltid användas som sökbegrepp. En sökning på namn eller personnummer ska emellertid inte leda till att all information i polisens brottsbekämpande verksamhet som rör den sökta personen omedelbart avslöjas. Utgångspunkten är att endast sådana uppgifter som det generellt sett finns ett behov av i polisens brottsbekämpande verksamhet får tas fram. I paragrafens *första stycke* finns en uttömmande uppräkning av de kategorier av personuppgifter som får tas fram vid sökning på namn, personnummer och andra liknande identitetsbeteckningar, dvs. vilka personuppgifter som får ingå i träffbilden vid en sådan sökning.

I *punkten 1* anges att sådana uppgifter som anger att den sökte är anmäld för brott får tas fram. Att personen ”är anmäld” innebär att avförda brottsanmälningar faller utanför. Som framgår av 10 § finns det begränsningar i fråga om behandlingen av vissa anmälningar. Uppgifter om personen kan trots detta vara tillgängliga om någon annan av punkterna är tillämplig, t.ex. punkten 2 eller 3. Av *punkten 2* framgår att uppgifter om att den sökte är eller tidigare har varit misstänkt för brott får tas fram. Det ska således framgå om brottsmisstanken fortfarande är aktuell eller om personen har avförts såsom misstänkt. Enligt *punkten 3* får även sådana uppgifter tas fram som anger att den sökta personen är misstänkt för att utöva eller komma att utöva brottslig verksamhet. I kommentaren till 4 § redogörs närmare för vad som avses med misstanke om brottslig verksamhet. Även uppgifter om att den sökta personen övervakas får enligt *punkten 4* ingå i träffbilden. Det är här fråga om uppgifter som anger att den sökta personen är föremål för övervakning på grund av att denne är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet (se kommentaren till 2 §). Vidare får, enligt *punkterna 5–8* uppgifter tas fram som anger att den sökta personen har gjort en brottsanmälan, är målsägande eller förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande. Detsamma gäller en person som har gett in eller tillhandahållits en handling. Av *punkten 9* följer att uppgifter som anger att den sökta personen är anmäld försvunnen får tas fram. För att polisen snabbt ska kunna vidta erforderliga åtgärder inför och i samband med ett ingripande får även uppgifter som anger att den sökta personen har bedömts kunna komma att möta ett polisingripande med grovt våld ingå i träffbilden. Detta regleras i *punkten 10*. I avsnitt 11.3 har redogjorts närmare för i vilka situationer en sådan bedömning kan bli aktuell. Enligt *punkten 11* får uppgifter om att den sökta personen är efterlyst tas fram. Det är här fråga om sådana efterlysningar som sker med stöd av efterlysningskungörelsen (1969:293) eller lagen (2000:344) om Schengens informationssystem.

Vid en sökning i gemensamt tillgängliga uppgifter på namn, personnummer eller liknande identitetsbeteckningar får det alltså inte tas fram uppgifter av annat slag, t.ex. uppgifter från underrättelsearbete som visar att den sökte är släkt med eller inneboende hos en övervakad person.

Med namn avses även delar av namn och med personnummer och samordningsnummer även de sifferkombinationer som ingår i numren. Också sökning med hjälp av födelsedatum eller de sista fyra kontrollsiffrorna i ett personnummer omfattas alltså av bestämmelsen. Bestämmelsen är avsedd att omfatta motsvarande nummer som används i andra länder även om de är uppbyggda på annat sätt.

Bestämmelsen ställer krav på utformningen av de tekniska system som används vid sökning. Vid sökning på ett visst namn, N.N., ska det i träffbilden inte komma upp andra uppgifter om N.N. än sådana som anges i paragrafen och uppgifter som har direkt anknytning till den egenskapen, t.ex. skälen till att en person är efterlyst eller uppgifter om den förundersökning i vilken personen förekommer. Bestämmelsen är dock inte avsedd att förhindra att det vid en sökning, som visar att N.N. är eller tidigare har varit misstänkt för visst brott, också går att ta del av annan, i anslutning till brottsmisstanken angiven information, t.ex. att N.N. är inneboende hos eller släkt med S.S. Ytterligare uppgifter om N.N. ska

således kunna tas fram genom fortsatt sökning, förutsatt att den som gör sökningen har rätt att få tillgång till uppgiften. Vid en sökning på en person som visserligen förekommer i de gemensamt tillgängliga uppgifterna men inte tillhör någon av de kategorier som anges i första stycket punkterna 1–11 ska det däremot inte komma fram någon information vid en initial sökning. Om det inte finns några andra uppgifter om S.S. än att han har N.N. som inneboende ska alltså en sökning på S.S. inte ge någon träff.

Möjligheten att vid en sökning få fram vissa typer av personuppgifter kan behöva begränsas ytterligare. Sådana personuppgifter som avses i punkterna 2–4, t.ex. uppgifter i nedlagda förundersökningar eller underrättelseinformation, är typiskt sett av mera integritetskänsligt slag. Det kan därför finnas skäl att begränsa tillgången till sådana uppgifter. I *andra stycket* erinras därför om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om ytterligare begränsningar av tillgången till sådana uppgifter. Att tillgången till personuppgifter i polisens brottsbekämpande verksamhet generellt ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter följer av 2 kap. 11 §.

I 7 § finns undantag från sökbegränsningen i paragrafen.

7 § Bestämmelsen i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller
2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Bestämmelsen i 6 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän och som görs

1. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, eller
2. för att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första och andra styckena.

Regeringen meddelar föreskrifter om ytterligare undantag från bestämmelserna i 6 §.

Paragrafen innehåller fyra undantag från sökbegränsningsregeln i 6 §. Motiven till dessa undantag har redovisats i avsnitt 11.3.

Enligt *första stycket 1* gäller 6 § inte vid sökning som sker i ett visst ärende eller en viss handling. Det handlar här om sökning i så begränsade informationsmängder att några egentliga integritetsrisker inte kan anses föreligga.

Av *första stycket 2* framgår att 6 § inte heller gäller vid sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet (t.ex. narkotikabrottslighet i en viss region) eller vissa kriminella grupperingar (t.ex. ett mc-gäng) och som enbart de som arbetar i undersökningen har fått rätt att ha åtkomst till. Även här är det fråga om sökning i en avgränsad uppgiftsmängd, i dessa fall i form av en särskild uppgiftssamling, där tillgången till uppgifterna har begränsats. Denna bestämmelse medger inte att en person med tillgång till flera uppgiftssamlingar kan söka sam-

tidigt i dessa med hjälp av någon form av sökverktyg eller dylikt. Sådan sökning kan dock vara tillåten enligt andra stycket. Uppgifter som ingår i sådana uppgiftssamlingar som nu avses kan inte alltid anses vara gemensamt tillgängliga (jfr kommentaren till 1 §). Om så inte är fallet, är bestämmelserna i 3 kap. över huvud taget inte tillämpliga på dem.

Paragrafens *andra stycke* innehåller ytterligare två undantag från bestämmelserna i 6 §. En första förutsättning för att något av dessa undantag ska vara tillämpligt är att sökningen utförs av särskilt angivna tjänstemän. Det är här fråga om på förhand utpekade tjänstemän som med hänsyn till tjänstebefattning, arbetsuppgifter eller dylikt har ett särskilt behov av att kunna utföra mera omfattande sökningar. Enligt *punkten 1* krävs därutöver att sökningen görs för att förebygga, förhindra eller upptäcka viss allvarlig brottslig verksamhet, eller för övervakning av vissa kriminella personer. Det är här fråga om sökning i underrättelseverksamhet som rör t.ex. grovt narkotikabrott, grov narkotikasmuggling, terroristbrott, människohandel, brott mot rikets säkerhet och andra grova brott. Punkten är även tillämplig på sökning som sker i samband med övervakning av personer som bedöms mer eller mindre livnära sig på brottslig verksamhet, t.ex. grov narkotikasmuggling eller människohandel (se kommentaren till 2 § första stycket punkten 2).

I *punkten 2* öppnas en möjlighet att, utan hinder av 6 §, göra mera omfattande sökningar även inom ramen för en förundersökning. I dessa fall krävs dock, utöver att sökningen utförs av särskilt angivna tjänstemän, att det är fråga om sökning i samband med utredning av mycket allvarliga brott, som t.ex. mord, eller seriebrott av allvarlig karaktär, t.ex. upprepade våldtäkter eller grova mordbränder. Avsikten är att sökmöjligheten främst ska utnyttjas under förundersökningens spaningsskede, innan det finns någon som är misstänkt för brottet.

De särskilt angivna tjänstemän som har möjlighet att göra sökningar enligt andra stycket har givetvis möjlighet att, på samma villkor som övriga tjänstemän, tillämpa undantagen i första stycket.

I *tredje stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter, t.ex. om att det ska framgå av en förteckning eller liknande vilka personer som har anförtrotts den utökade möjligheten att söka enligt andra stycket.

Av *fjärde stycket* följer att regeringen har möjlighet att meddela föreskrifter om ytterligare undantag från sökbegränsningarna i 6 §.

Direktåtkomst

8 § Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Paragrafen innehåller bestämmelser om direktåtkomst. Frågor om direktåtkomst har behandlats i avsnitt 12.1 och 12.3. Innebörden av begreppet direktåtkomst redovisas i kommentaren till 2 kap. 21 §.

I *första stycket* anges att Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Som utvecklas i kommentaren till 2 kap. 16 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst.

Bestämmelsen innebär inte att de i paragrafen angivna myndigheterna har en absolut rätt till direktåtkomst. En bestämmelse om direktåtkomst anger endast i vilken form uppgifter får lämnas ut. Möjligheten att lämna ut vissa uppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Något utlämnande genom direktåtkomst får normalt inte ske om utlämnandet förutsätter en sekretessprövning. I och med att Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndighetens polisiära verksamhet i 2 kap. 16 § åläggs en sekretessbrytande uppgiftsskyldighet i förhållande till varandra och andra brottsbekämpande myndigheter kan dock uppgifter som omfattas av den bestämmelsen utlämnas genom direktåtkomst.

Av *andra stycket* framgår att om en myndighet har beviljats direktåtkomst till personuppgifter som behandlas enligt lagen, ansvarar denna för att tillgången till uppgifterna inom den egna myndigheten begränsas. I polisens verksamhet gäller samma krav på begränsning enligt 2 kap. 11 §, oavsett på vilket sätt man fått tillgång till uppgifterna. Andra myndigheter som beviljats direktåtkomst, exempelvis Tullverket och Åklagarmyndigheten, ska iaktta kravet i förevarande paragraf. Myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften.

I *tredje stycket* informeras om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om bl.a. begränsningar i direktåtkomsten och om behörighet och säkerhet. Med utgångspunkt i paragrafens bestämmelser och eventuella föreskrifter får varje myndighet avgöra om den kan medge en annan myndighet direktåtkomst.

Bevarande av personuppgifter i ärenden om utredning eller beivrande av brott

9 § I 10–12 §§ anges hur länge personuppgifter i vissa ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga längst får bevaras i polisens brottsbekämpande verksamhet.

Paragrafen, som har behandlats i avsnitt 14.4, anger ramarna för behandlingen av personuppgifter i vissa avslutade ärenden om utredning och beivrande av brott.

En utgångspunkt är att ärenden om utredning eller beivrande av brott inte ska gallras enligt lagens bestämmelser (jfr 2 kap. 13 § andra stycket). För gemensamt tillgängliga uppgifter i vissa sådana ärenden föreskrivs dock i 10–12 §§ – i stället för gallringsregler – en längsta tid för bevarande. Bestämmelserna kompletterar den generella bestämmelsen om bevarande i 2 kap. 12 § första stycket. Bestämmelserna i 10–12 §§ reglerar

bevarandet av uppgifter i brottsanmälningar, avslutade förundersökningar och andra utredningar som handläggs enligt 23 kap. rättegångsbalken. Dessa kategorier utgör huvuddelen av de uppgifter som behandlas för ändamålet att utreda eller beivra brott. Eftersom det emellertid förekommer ärenden om utredning eller beivrande av brott som inte tillhör någon av de nu nämnda kategorierna, t.ex. ärenden om ändring av påföljd eller yttranden angående verkställighet av rättspsykiatrisk vård med särskild utskrivningsprövning, anges att bestämmelserna avser vissa sådana ärenden.

Bestämmelserna om längsta tid för bevarande hindrar inte att handlingar arkiveras och gallras enligt arkivlagens (1990:782) bestämmelser. När behandling inte längre är tillåten för brottsbekämpande ändamål kan bevarande således ske för arkivändamål. Med hänsyn till att arkivering kan ske digitalt och att arkivering i sig inte utesluter fortsatt digital tillgång till uppgifter i verksamheten, kan regeringen, i syfte att begränsa tillgången till uppgifterna, meddela föreskrifter om digital arkivering (se kommentaren till 2 kap. 12 § tredje stycket).

10 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas i polisens brottsbekämpande verksamhet efter det att åtal inte längre får väckas för brottet.

Paragrafen, som har behandlats i avsnitt 14.4, reglerar hur länge personuppgifter i en brottsanmälan får behandlas, i de fall där anmälan i fråga inte har lett till en förundersökning eller annan motsvarande utredning. För anmälningar som resulterat i förundersökning eller annan utredning gäller i stället bestämmelserna i 11 §.

Huvudregeln är att uppgifter i en avskriven brottsanmälan ska kunna behandlas fram till den tidpunkt när brottet preskriberas, eftersom förundersökning kan inledas om det kommer fram omständigheter som gör att brottet kan klaras upp. När brottet inte längre kan bli föremål för åtal, får uppgifterna däremot inte behandlas längre i den brottsbekämpande verksamheten. Motsvarande gäller om brottet är preskriberat redan när anmälan görs.

Från huvudregeln om att behandling får ske fram till dess att brottet har preskriberats görs dock undantag för uppgifter i sådana anmälningar som har avskrivits på den grunden att det inte förelåg något brott, exempelvis anmälningar som gäller icke straffbara gärningar. Det kan t.ex. vara fråga om en brand som hade naturliga orsaker, ett handlande som inte är straffbelagt eller något annat som inte utgör brott. Uppgifter i sådana anmälningar får, när beslut om avskrivning har meddelats, inte behandlas i den brottsbekämpande verksamheten.

11 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då domen, eller det beslut som meddelades med anledning av talan, vann laga kraft.

Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas i polisens brotts-

bekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

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

Paragrafen, som har behandlats i avsnitt 14.4, reglerar hur lång tid personuppgifter i avslutade förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken längst får behandlas i den brottsbekämpande verksamheten. Utgångspunkten är att brottsutredningar ska kunna behandlas viss tid efter det att ärendet avslutades. En förutsättning för behandlingen är dock att uppgifterna behöver bevaras för något eller några av lagens ändamål (se kommentaren till 2 kap. 12 §). Eftersom det kan vara fråga om betydande mängder information, har det av integritetsskäl bestämts en yttersta tidsgräns om fem år för sådan fortsatt behandling.

Första stycket behandlar förundersökningar som har lett till åtal eller annan domstolsprövning (t.ex. särskild förverkandetalan). I fråga om sådana förundersökningar räknas tiden om fem år från utgången av det kalenderår då domstolens dom eller slutliga beslut vann laga kraft.

I *andra stycket* regleras förundersökningar som inte har lett till domstolsprövning. Hit hör bl.a. nedlagda förundersökningar och förundersökningar om brott som lagförts genom strafföreläggande. I dessa fall räknas femårsfristen från utgången av det kalenderår då förundersökningen avslutades.

Bestämmelserna i paragrafen hindrar inte att uppgifter från en brottsanmälan eller förundersökning fram till femårsfristens utgång inhämtas till annan brottsbekämpande verksamhet, t.ex. ett särskilt underrättelseprojekt, under förutsättning att de behövs där (2 kap. 7 §). I dessa fall får uppgifterna fortsätta att behandlas för sitt nya ändamål även sedan den ursprungliga fristen har gått ut. En sådan behandling får dock bara ske i den utsträckning behandlingen behövs för det nya ändamålet. Vidare förutsätts att uppgifterna då gallras från den brottsbekämpande verksamheten enligt de bestämmelser som gäller för behandlingen för det nya ändamålet. Om det t.ex. är ett underrättelseprojekt ska uppgiften gallras enligt bestämmelserna i 14 §. Denna grundläggande princip, att ändamålet för behandlingen är avgörande för hur länge en viss uppgift får bevaras, berörs även i kommentaren till 14 §.

Bestämmelserna i paragrafen gäller, som framgår av *tredje stycket*, också uppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. Vad som avses med ”annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken” behandlas i kommentaren till 2 kap. 7 §.

Av 12 § framgår att regeringen får meddela föreskrifter om att vissa kategorier av personuppgifter får bevaras under längre tid än vad som anges i denna paragraf.

12 § Regeringen meddelar föreskrifter om att vissa kategorier av personuppgifter får bevaras i polisens brottsbekämpande verksamhet under längre tid än vad som anges i 10 och 11 §§.

Av paragrafen framgår att regeringen får meddela föreskrifter om att vissa kategorier av personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken får bevaras under längre tid än vad som anges i 10 och 11 §§. Frågan har behandlats i avsnitt 14.4.

Regeringen har möjlighet att meddela föreskrifter om att vissa kategorier av uppgifter från framför allt förundersökningar, exempelvis uppgifter om gods, får bevaras under längre tid än fem år. Sådana föreskrifter kan t.ex. även avse uppgifter om särskilda tillvägagångssätt vid brott, s.k. modus operandi. Det kan vidare vara fråga om fortsatt behandling av uppgifter om dömda personer, t.ex. personer som förekommer i belastningsregistret, i syfte att förenkla för polisen att hitta ärenden som har arkiverats.

13 § Om en förundersökning mot en person 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.

Paragrafen innehåller en bestämmelse om behandling av personuppgifter som rör brottsmisstankar efter det att en förundersökning har lagts ned, ett åtal har lagts ned eller en åtalad person har frikänts genom en lagakraftvunnen dom. Bestämmelsen har motiverats i avsnitt 14.4.

Enligt paragrafen får en person inte vara sökbar som misstänkt efter det att förundersökningen mot personen har lagts ned. Detta gäller oavsett skälet för nedläggningsbeslutet. Om förundersökningen har lett till åtal, men detta har lagts ned eller lett till en frikännande dom, får den åtalade personen på motsvarande sätt inte längre vara sökbar som misstänkt för brottet.

Bestämmelsen ska inte tolkas så att alla handlingar där det förekommer uppgifter om att en viss person har pekats ut eller hörts som misstänkt måste förstöras. Däremot ska det inte längre vara möjligt att vid sökning i elektroniskt lagrat material återfinna den utpekade personen om man söker efter misstänkta personer. Bestämmelsen utesluter således inte att det vid en sökning kommer fram uppgifter om en person som tidigare har varit misstänkt, förutsatt att det framgår att han eller hon inte längre är misstänkt för brottet i fråga.

Bestämmelsen begränsar alltså inte fortsatt behandling av andra personuppgifter avseende den tidigare misstänkta personen än själva misstanken om brott. Om förundersökningen om brottet fortsätter, är det givetvis också tillåtet att behandla misstankar mot andra personer.

Bevarande och gallring av övriga personuppgifter

14 § Personuppgifter som har gjorts gemensamt tillgängliga enligt 2 § första stycket 1, 2, 4 eller 5 ska gallras enligt bestämmelserna i andra–sjätte styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Uppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver ska dock gallras senast fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personen

görs före utgången av gallringsfristen, behöver de uppgifter som finns om personen inte gallras så länge någon av uppgifterna om honom eller henne får bevaras.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Uppgifter som har behandlats med stöd av 2 § första stycket 4 ska gallras senast ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Uppgifter som har behandlats med stöd av 2 § första stycket 5 ska gallras senast ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Den tid då en misstänkt eller övervakad person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i andra och tredje styckena.

Paragrafen innehåller bestämmelser som, tillsammans med 15 §, reglerar gallring av andra gemensamt tillgängliga uppgifter än uppgifter i ärenden om utredning eller beivrande av brott. Enligt *första stycket* ska vid gallring av nu aktuella uppgifter 14 och 15 §§ tillämpas i stället för bestämmelserna i 2 kap. 13 §. Bakgrunden till bestämmelserna har utvecklats i avsnitt 14.3. I avsnitt 14.1 har kommenterats vad som avses med gallring.

Det gäller olika gallringsfrister beroende på vilket slag av uppgifter det är fråga om.

Enligt *andra stycket* ska personuppgifter som kan antas ha samband med misstänkt brottslig verksamhet gallras senast efter tre år om den misstänkta verksamheten innefattar brott för vilket är föreskrivet fängelse i ett år eller som sker systematiskt. Om den misstänkta verksamheten innefattar brott för vilket är föreskrivet fängelse i två år eller däröver gäller i stället en femårig gallringsfrist. Fristerna räknas från utgången av det kalenderår då registreringen avseende en person gjordes. Om ytterligare uppgifter om personen samlas in – oavsett om de har samband med den brottsliga verksamhet som först föranledde registrering eller annan brottslig verksamhet – förlängs gallringsfristen med tre eller fem år beroende på hur allvarlig den nya brottsliga verksamheten är. Med personuppgifter avses såväl direkta som indirekta personuppgifter, dvs. inte bara uppgifter som direkt tar sikte på en person, t.ex. namn och utseende, utan också uppgifter om fordon, adresser m.m. som kan knytas till en person. Som framgår av sjätte stycket kan fristen påverkas av frihetsberövanden.

Tredje stycket innehåller bestämmelser om gallring av uppgifter som behandlas i samband med övervakning av brottsbelastade eller potentiellt farliga personer, dvs. med stöd av 2 § första stycket 2. Sådana uppgifter ska gallras inom tio år från utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Som framgår av sjätte stycket kan fristen påverkas av frihetsberövanden.

I *fjärde stycket* anges att uppgifter som har behandlats med stöd av 2 § första stycket 4, dvs. uppgifter som behövs för att fullgöra internationella åtaganden, ska gallras senast ett år efter utgången av det kalenderår då det ärende i vilket uppgifterna behandlades avslutades. Bestämmelsen ska tillämpas t.ex. när en svensk brottsbekämpande myndighet har lämnat rättslig hjälp åt en utländsk myndighet.

Enligt *femte stycket* ska uppgifter som har behandlats med stöd av 2 § första stycket 5, dvs. uppgifter som har rapporterats till polisens kommunikationscentraler, gallras senast ett år efter utgången av det kalenderår då uppgifterna behandlades automatiserat första gången.

Gallringsfristerna i andra–femte styckena utgör maximitider. I den mån det redan vid en tidigare tidpunkt står klart att uppgifterna saknar betydelse från brottsbekämpningssynpunkt ska de gallras redan då. Detta följer av ändamålsbestämmelserna i 2 kap. 7 § och den generella bestämmelsen om längsta tid för bevarande i 2 kap. 12 § första stycket.

En uppgift som samlats in för ett visst ändamål kan senare komma att behandlas för ett nytt ändamål. Om det exempelvis – innan gallring har skett – uppkommer behov av uppgifter som behandlas i ett underrättelseprojekt i någon annan brottsbekämpande verksamhet, t.ex. vid övervakning av viss person, får uppgifterna hämtas in till den verksamheten. I så fall gäller en ny gallringsfrist för det nya ändamålet. Detsamma gäller om en uppgift som har rapporterats till en kommunikationscentral senare behandlas i en förundersökning.

Av *sjätte stycket* framgår att den tid som en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning inte räknas med vid beräkningen av gallringsfristerna i andra och tredje styckena. Bestämmelsen tar endast sikte på misstänkta eller övervakade personer.

15 § Regeringen meddelar föreskrifter om att vissa kategorier av personuppgifter får bevaras under längre tid än vad som anges i 14 §.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 14 §, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Frågan har behandlats i avsnitt 14.1. Av paragrafens *första stycke* framgår att regeringen har möjlighet att meddela föreskrifter om att uppgifter får bevaras längre än vad som följer av 14 §. En motsvarande bestämmelse som gäller uppgifter i ärenden om utredning eller beivrande av brott finns i 12 §. Regeringen kan således föreskriva att speciella slag av uppgifter ska gallras först efter längre tid.

Av *andra stycket* följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att personuppgifter, trots gallringsbestämmelserna, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

4 kap. Register

Register över DNA-profiler

Ändamål

1 § Rikspolisstyrelsen får föra register över DNA-profiler (DNA-registret, utredningsregistret och spårregistret) i enlighet med 2–10 §§. Dessa register får även föras för att underlätta identifiering av avlidna personer.

Paragrafen reglerar vilka register över DNA-profiler som får föras och för vilka ändamål. Frågan har behandlats i avsnitt 15.2. Av 3 kap. 2 §

andra stycket följer att DNA-profiler inte får göras gemensamt tillgängliga. I den bestämmelsen tydliggörs att sådana uppgifter får behandlas i särskilda register med stöd av bestämmelser i detta kapitel.

Endast Rikspolisstyrelsen får föra register över DNA-profiler. Begreppet ”DNA-profiler” har ersatt uttrycket ”uppgifter om resultatet av DNA-analyser” som används i 22 § polisdatalagen (1998:622). Vad som avses med DNA-profil utvecklas i kommentaren till 2 kap. 3 §. Förändringen tydliggör att det är DNA-profilen, som inte innehåller någon information om den registrerades personliga egenskaper, som registreras. Vidare benämns, i förtydligande syfte, de tre DNA-registren (DNA-registret, utredningsregistret och spårregistret) i bestämd form.

Registren får föras dels för de ändamål som anges i 2 kap., dels för att underlätta identifiering av avlidna personer. Registrens närmare innehåll regleras i 2–5 §§.

DNA-registret

2 § DNA-registret får innehålla DNA-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller
2. har godkänt ett strafföreläggande som avser villkorlig dom.

Paragrafen, som tillsammans med 3 § reglerar innehållet i DNA-registret, överensstämmer i huvudsak med 23 § polisdatalagen (1998:622). Frågan har behandlats i avsnitt 15.2. I paragrafen har en förändring gjorts med anledning av definitionen i 2 kap. 3 § av begreppet DNA-profil (jfr kommentaren till denna paragraf). Härigenom tydliggörs att det är DNA-profilen som registreras och utgör det primära innehållet i registret. Vidare har benämningen på registret ändrats till bestämd form i konsekvens med ändringen i 1 §.

3 § En DNA-profil som registreras får endast ge information om identitet och inte om personliga egenskaper.

Utöver DNA-profiler får DNA-registret innehålla uppgifter om vem analysen avser och i vilket ärende DNA-profilen har tagits fram samt brottskod.

Paragrafen, som har behandlats i avsnitt 15.2, reglerar tillsammans med 2 § DNA-registrets innehåll. Den överensstämmer i huvudsak med 24 § polisdatalagen (1998:622). Förändringarna är av samma slag som i 2 §. Vidare har det tydliggjorts att uppgifter om brottskoder får antecknas i registret. Med brottskod avses den kod som används för att framställa brottsstatistik och som anger vilket brott som den aktuella personen är misstänkt eller dömd för.

Utredningsregistret

4 § Utredningsregistret får innehålla DNA-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket fängelse kan följa.

Bestämmelserna i 3 § gäller också vid registrering i utredningsregistret.

Paragrafen, som reglerar innehållet i utredningsregistret, överensstämmer i huvudsak med 24 a § polisdatalagen (1998:622). Förändringarna är av samma slag som i 2 §.

Spårregistret

5 § Spårregistret får innehålla DNA-profiler som har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver DNA-profiler får spårregistret innehålla upplysningar som visar i vilket ärende analysen har gjorts och brottskod.

Paragrafen, som reglerar vad spårregistret får innehålla, överensstämmer i huvudsak med 25 § polisdatalagen (1998:622). Ändringarna är av samma slag som i 2 §. Vidare har det tydliggjorts att uppgifter om brottskoder får antecknas i registret. Med brottskod avses den kod som används för att framställa brottsstatistik och som anger vilket brott som den aktuella misstanken avser.

6 § DNA-profiler i spårregistret får jämföras med DNA-profiler

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

DNA-profiler i spårregistret får också jämföras i andra fall om det är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Paragrafen innehåller bestämmelser som begränsar användningen av uppgifter i spårregistret, som enbart innehåller DNA-profiler från oidentifierade personer. Frågan har behandlats i avsnitt 15.2.

Första stycket överensstämmer i huvudsak med 26 § polisdatalagen (1998:622). Förändringarna är av samma slag som i 2 §.

Enligt *andra stycket* får DNA-profiler jämföras med uppgifter i spårregistret om ett internationellt åtagande kräver det. Ett sådant finns i Prümrådsbeslutet (avsnitt 4.4.3). Enligt detta ska andra staters oidentifierade DNA-profiler automatiskt kunna jämföras med de DNA-profiler som finns i det svenska spårregistret.

Gallring

7 § Uppgifter i DNA-registret ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i utredningsregistret ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter i spårregistret ska gallras senast trettio år efter registreringen. Sådana uppgifter ska dock gallras senast sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om

1. mord eller dråp enligt 3 kap. 1 eller 2 § brottsbalken,
2. folkrättsbrott enligt 22 kap. 6 § andra stycket brottsbalken,
3. folkmord enligt 1 § lagen (1964:169) om straff för folkmord,

4. terroristbrott enligt 3 § 1 eller 2 jämförd med 2 § lagen (2003:148) om straff för terroristbrott, eller

5. försök till brott som avses i 1, 3 eller 4.

Paragrafen innehåller bestämmelser om gallring av uppgifter i de olika registren över DNA-profiler. Frågan har behandlats i avsnitt 15.2.

Första och *andra styckena* överensstämmer i sak med motsvarande stycken i 27 § polisdatalagen (1998:622). Några smärre språkliga ändringar har gjorts.

I det *tredje stycket* regleras gallring i spårregistret. Enligt huvudregeln ska uppgifter i registret gallras senast trettio år efter registreringen. Undantag görs för uppgifter som hänför sig till utredningar om vissa brott. Det rör sig om sådana brott som reglerna om preskription inte är tillämpliga på enligt förslaget om ändring i 35 kap. 2 § brottsbalken i lagrådsremissen Preskription för allvarliga brott. Då ska uppgifterna i stället gallras senast sjuttio år efter registreringen

Prover för DNA-analys

8 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys, får provet inte användas för något annat ändamål än det som provet togs för.

Paragrafen, som begränsar användningen av prov som tagits för DNA-analys, överensstämmer med 28 § polisdatalagen (1998:622). Begreppet DNA-analys definieras i 2 kap. 3 §, se kommentaren till den paragrafen. Provtagning för DNA-analys regleras i 28 kap. rättegångsbalken.

9 § Ett prov för DNA-analys som har tagits med stöd av 28 kap. rättegångsbalken, eller på begäran av annan stat, ska förstöras senast sex månader efter det att provet togs.

Paragrafen, som reglerar när DNA-prover ska förstöras, har behandlats i avsnitt 15.2. Det rör sig om prover som har tagits på personer med stöd av bestämmelserna om kroppsbesiktning i 28 kap. rättegångsbalken eller på begäran av annan stat. Paragrafen överensstämmer delvis med 27 a § polisdatalagen (1998:622).

En enhetlig tidsgräns för när DNA-prov ska förstöras har införts. Den omfattar såväl prov som har tagits enligt bestämmelserna om förundersökning som motsvarande prov som har tagits på begäran av en annan stat. Ett prov för DNA-analys ska enligt paragrafen förstöras senast sex månader efter det att provet togs.

Direktåtkomst

10 § Polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Statens kriminaltekniska laboratorium får medges direktåtkomst till register över DNA-profiler.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Skälen för den valda lösningen har redovisats i avsnitt 12.3.3 och 12.3.4.

Enligt *första stycket* får polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Statens kriminaltekniska laboratorium medges direktåtkomst till DNA-registren (dvs. DNA-registret, utredningsregistret och spårregistret). Som anges i kommentaren till 2 kap. 16 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst. Regleringen överensstämmer, utom vad avser Tullverket och Kustbevakningen, med 11 § polisdataförordningen (1999:81). I kommentaren till 2 kap. 21 § redogörs för vad som avses med direktåtkomst.

Av *andra stycket* framgår att om en myndighet har beviljats direktåtkomst till personuppgifter som behandlas enligt lagen, ansvarar denna för att tillgången till uppgifterna inom den egna myndigheten begränsas. I polisens verksamhet gäller samma krav på begränsning enligt 2 kap. 11 §, oavsett på vilket sätt man fått tillgång till uppgifterna. Andra myndigheter som beviljats direktåtkomst, exempelvis Tullverket och Åklagarmyndigheten, ska iaktta kravet i förevarande paragraf. Myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften.

Enligt 11 § polisdataförordningen ska annan myndighet än Statens kriminaltekniska laboratorium endast ha tillgång till uppgifter om huruvida någon förekommer i ett register eller inte. I paragrafens *tredje stycke* informeras om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter, som bl.a. kan avse motsvarande begränsning.

Se kommentaren till 2 kap. 21 § angående utländska myndigheters direktåtkomst till DNA-register.

Fingeravtrycks- eller signalementsregister

Ändamål

11 § Rikspolisstyrelsen får föra fingeravtrycks- eller signalementsregister i enlighet med 12–17 §§. Dessa register får även föras för att underlätta identifiering av okända personer.

I paragrafen anges att Rikspolisstyrelsen får föra sådana fingeravtrycks- eller signalementsregister vilkas innehåll preciseras i 12 och 13 §§. Frågan har behandlats i avsnitt 15.3. Förutom för de ändamål som anges i 2 kap. får registren föras för att underlätta identifiering av okända personer. Fingeravtrycks- eller signalementsregister utgör ett stöd framför allt i den brottsutredande verksamheten men kan användas även för att underlätta arbetet med att förebygga och förhindra brott.

12 § I fingeravtrycks- eller signalementsregister får uppgifter behandlas om en person som

1. är misstänkt eller dömd för brott och som har varit föremål för åtgärd enligt 28 kap. 14 § rättegångsbalken, eller
2. har lämnat fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll.

Uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person får behandlas om uppgiften kommit fram i en utredning om brott.

Uppgifter om fingeravtryck får även behandlas om det behövs för att fullgöra internationella åtaganden.

I fingeravtrycks- eller signalementsregister får inte uppgifter behandlas som har lämnats av en person under femton år enligt 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Skälen för paragrafens bestämmelser har behandlats i avsnitt 15.3. Bestämmelserna motsvarar delvis 30 § polisdatalagen (1998:622).

I *första stycket* har förtydligats att registren består av fingeravtryck och fotografier m.m. som tagits med stöd av 28 kap. 14 § rättegångsbalken och som tillsammans med personens signalement skickats till Rikspolisstyrelsen enligt 7 § förordningen (1992:824) om fingeravtryck m.m.

Enligt *andra stycket* får sådana uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person och som har säkrats vid utredning av brott behandlas. Genom bestämmelsen klargörs att spår från brottsplatser får behandlas i registret.

Av *tredje stycket* framgår att uppgifter även får behandlas om det behövs för att fullgöra ett internationellt åtagande. Det kan exempelvis vara fråga om att registrera ett oidentifierat fingeravtryck som Sverige erhållit från ett annat land.

Fjärde stycket motsvarar 30 § andra stycket polisdatalagen.

13 § Fingeravtrycks- eller signalementsregister får innehålla uppgifter om

1. fingeravtryck,
2. signalement,
3. fotografi,
4. videoupptagning,
5. identifieringsuppgifter,
6. ärendenummer, och
7. brottskod.

Paragrafen reglerar tillsammans med 12 § innehållet i fingeravtrycks- eller signalementsregister. Den innehåller en uttömmande uppräkning av vilka uppgifter som får behandlas. Skälen för paragrafens bestämmelser har behandlats i avsnitt 15.3.

Paragrafen motsvarar delvis 30 § polisdatalagen (1998:622). Begreppet fingeravtryck i *punkten 1* definieras i 2 kap. 3 §. Det omfattar avtryck av fingrar och hand. *Punkterna 2, 5* och *6* är desamma som i 30 § polisdatalagen. I uppräkningen av vilka kategorier av uppgifter som fingeravtrycks- eller signalementsregister får innehålla har *punkterna 3, 4* och *7* lagts till. Det innebär att även fotografier, videoupptagningar och brottskoder får finnas i registren. Med brottskod avses den kod som används

för att framställa brottsstatistik och som anger vilket brott som den aktuella misstanken avser.

Gallring

14 § Uppgifter i fingeravtrycks- eller signalementsregister om en misstänkt person ska gallras senast tre månader efter att uppgifter om personen gallrats ur misstankeregistret som förs enligt lagen (1998:621) om misstankeregister och ur belastningsregistret som förs enligt lagen (1998:620) om belastningsregister.

Uppgifter som inte kan hänföras till en identifierbar person ska gallras senast trettio år efter registreringen. Sådana uppgifter ska dock gallras senast sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om

1. mord eller dråp enligt 3 kap. 1 eller 2 § brottsbalken,
2. folkrättsbrott enligt 22 kap. 6 § andra stycket brottsbalken,
3. folkmord enligt 1 § lagen (1964:169) om straff för folkmord,
4. terroristbrott enligt 3 § 1 eller 2 jämförd med 2 § lagen (2003:148) om straff för terroristbrott, eller
5. försök till brott som avses i 1, 3 eller 4.

Paragrafen reglerar gallring av uppgifter i fingeravtrycks- eller signalementsregister som behandlas med stöd av 12 § första stycket 1 och andra stycket. Frågan har behandlats i avsnitt 15.3.

Enligt *första stycket* ska uppgifter om en misstänkt person gallras senast tre månader efter det att uppgifter om personen inte längre förekommer i vare sig misstankeregistret eller belastningsregistret.

I *andra stycket* regleras gallringen av sådana fingeravtryck från oidentifierade personer som har säkrats i en brottsutredning, dvs. spår från en brottsplats. Sådana uppgifter ska enligt huvudregeln gallras senast trettio år efter registreringen. Undantag görs för uppgifter som hänför sig till utredningar om vissa brott. Det rör sig om sådana brott som reglerna om preskription inte är tillämpliga på enligt förslaget om ändring i 35 kap. 2 § brottsbalken i lagrådsremissen Preskription för allvarliga brott. Då ska uppgifterna i stället gallras senast sjuttio år efter registreringen. Regleringen motsvarar vad som enligt 7 § gäller för oidentifierade DNA-spår.

15 § Uppgifter i fingeravtrycks- eller signalementsregister som behandlas för att fullgöra ett internationellt åtagande ska gallras när uppgifterna inte längre behövs för ändamålet med behandlingen.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll ska gallras senast tio år efter registreringen.

I paragrafen anges gallringsfrister för uppgifter i fingeravtrycks- eller signalementsregister som behandlas med stöd av 12 § första stycket 2 och tredje stycket. Frågan har behandlats i avsnitt 15.3.

I *första stycket* anges när uppgifter som behandlas för att fullgöra internationella åtaganden ska gallras. Sådana uppgifter ska gallras när de inte längre behövs för ändamålet med behandlingen, t.ex. när en förfrågan från en annan stat har besvarats och det inte längre finns något behov av uppgiften.

Gallring av uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll regleras i *andra stycket*. Uppgifterna ska gallras senast tio år efter registreringen.

16 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 14 och 15 §§, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Av paragrafen följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att uppgifter, trots gallringsbestämmelserna i 14 och 15 §§, får bevaras för historiska, statistiska eller vetenskapliga ändamål. Frågan har behandlats i avsnitt 15.3.

Direktåtkomst

17 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen, Skatteverket och Statens kriminaltekniska laboratorium får medges direktåtkomst till personuppgifter i fingeravtrycks- eller signalementsregister.

En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Enligt *första stycket* får, med undantag för Åklagarmyndigheten, brottsbekämpande myndigheter och Statens kriminaltekniska laboratorium medges direktåtkomst till fingeravtrycks- eller signalementsregister. Åklagare har inte bedömts ha behov av annat än enstaka uppgifter ur aktuella register och finns därför inte med i uppräkningen. Som anges i kommentaren till 2 kap. 16 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst. Frågan har behandlats i avsnitt 12.3.3 och 12.3.4.

Av *andra stycket* framgår att om en myndighet har beviljats direktåtkomst till personuppgifter som behandlas enligt lagen, ansvarar denna för att tillgången till uppgifterna inom den egna myndigheten begränsas. I polisens verksamhet gäller samma krav på begränsning enligt 2 kap. 11 § oavsett på vilket sätt man fått tillgång till uppgifterna. Andra myndigheter som beviljats direktåtkomst, exempelvis Tullverket, ska iaktta kravet i förevarande paragraf. Myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften.

I *tredje stycket* informeras om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter. Regeringen kan t.ex. föreskriva att endast polispersonal vid Ekobrottsmyndigheten ska medges åtkomst till uppgifter ur registret. Vidare kan det meddelas föreskrifter om andra begränsningar i fråga om åtkomst och om behörighet och säkerhet.

Se kommentaren till 2 kap. 21 § angående utländska myndigheters direktåtkomst till fingeravtrycks- eller signalementsregister.

Penningtvättsregister

Ändamål

18 § Rikspolisstyrelsen får behandla personuppgifter i penningtvättsregister om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet

1. där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller
2. som innefattar finansiering av terrorism.

Enligt paragrafen, som anger ändamålen för penningtvättsregister, får Rikspolisstyrelsen behandla uppgifter i särskilda penningtvättsregister inom ramen för arbetet med att bekämpa penningtvätt och finansiering av terrorism. Frågan har behandlats i avsnitt 15.4.

Uppgifter får behandlas i sådana register om det behövs för att förebygga, förhindra eller upptäcka vissa slag av brottslig verksamhet. I *punkten 1* avses sådan brottslig verksamhet där penningtvätt utgör ett led för att dölja vinning av brott eller brottslig verksamhet. I *punkten 2* avses brottslig verksamhet som innefattar finansiering av terrorism. Begreppen penningtvätt och finansiering av terrorism definieras i 1 kap. 5 § 4 och 6 lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism. I denna paragraf används begreppen med samma innebörd.

19 § I ett penningtvättsregister får personuppgifter behandlas som

1. kan antas ha samband med sådan brottslig verksamhet som avses i 18 §,
2. har rapporterats till Rikspolisstyrelsen med stöd av bestämmelser i lag eller annan författning, eller
3. har lämnats av en utländsk myndighet som i sin stat ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i 18 §.

I paragrafen, som har behandlats i avsnitt 15.4, anges vilka personuppgifter som får behandlas i ett penningtvättsregister. Paragrafen innehåller en uttömmande uppräkning av vilka uppgifter som får behandlas.

Enligt *punkten 1* får polisen behandla uppgifter som har samband med sådan brottslig verksamhet som anges i 18 §, dvs. penningtvätt och terrorismfinansiering. I kommentaren till 3 kap. 2 § första stycket 1 utvecklas vad som avses med att en uppgift ”kan antas ha samband med” och vad som avses med ”brottslig verksamhet”.

Uppgifter som har rapporterats till Rikspolisstyrelsen med stöd av lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) eller annan författning får enligt *punkten* 2 också behandlas i penningtvättsregister. Enligt penningtvättslagen är fysiska och juridiska personer som driver viss typ av verksamhet skyldiga att bl.a. granska misstänkta ekonomiska transaktioner och att till polisen lämna uppgifter om alla omständigheter som kan tyda på penningtvätt eller finansiering av terrorism. Även tillsynsmyndigheter som vid en inspektion eller på annat sätt upptäcker en omständighet som kan ha samband med eller utgöra penningtvätt eller finansiering av terrorism, ska enligt penningtvättslagen underrätta polisen om detta. Sådana anmälningar och rapporter får alltså behandlas med stöd av punkten 2. Detta gäller även om innehållet inte ger tillräckligt underlag för misstanke om brott eller brottslig verksamhet.

Vidare får enligt *punkten 3* sådana uppgifter behandlas som har rapporterats av utländska myndigheter som har motsvarande uppgifter som den svenska Finanspolisen.

Gallring

20 § Personuppgifter i ett penningtvättsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

I *första stycket* anges att personuppgifter ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Bestämmelsen, som har behandlats i avsnitt 15.4, knyter an till de regler om bevarande av uppgifter som finns i lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism. Gallringsfristen om fem år är en maximitid. Det generella kravet på att uppgifter ska gallras när de inte längre behövs i verksamheten gäller även för uppgifter i penningtvättsregister.

Av *andra stycket* följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att uppgifter, trots vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Det internationella registret

Ändamål

21 § Rikspolisstyrelsen får behandla personuppgifter i det internationella registret om det behövs för handläggningen av ärenden som rör internationellt polisiärt samarbete eller internationellt straffrättsligt samarbete.

Uppgifter angående dödsfall, olyckshändelser eller andra liknande händelser i utlandet får också behandlas i det internationella registret, om ärendet rör en fråga som ska handläggas av polisen.

Enligt paragrafen får Rikspolisstyrelsen behandla personuppgifter i ett särskilt internationellt register, vars syfte är att underlätta handläggningen av internationella ärenden av olika slag. Frågan har behandlats i avsnitt 15.5.

Enligt *första stycket* får Rikspolisstyrelsen för det första behandla personuppgifter i det internationella registret i syfte att ta emot, hantera, vidarebefordra och besvara förfrågningar och framställningar om internationellt polisiärt samarbete bl.a. inom ramen för samarbetet inom Europol och Interpol. Under bestämmelsen faller exempelvis samarbete med stöd av lagen (2000:343) om internationellt polisiärt samarbete och lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar. Det kan t.ex. vara fråga om internationell efterlysning av personer eller gods, kontakter rörande kontrollerade leveranser av narkotika, begäran om hjälp med förhör, delgivning eller annat samarbete. För det andra får uppgifter behandlas i registret om den svenska polisen eller någon

annan svensk brottsbekämpande myndighet begär internationellt polisiärt samarbete eller straffrättsligt samarbete av andra stater och begäran kommuniceras via Rikspolisstyrelsen. Genom att straffrättsligt samarbete ingår i uppräkningen markeras att även sådana framställningar från andra svenska myndigheter som bl.a. åklagare och domstolar som endast befordras av polisen till myndigheter i andra länder får registreras. För det tredje fungerar Rikspolisstyrelsen som svensk kontaktpunkt och mottagare av information i det brottsbekämpande arbetet enligt en rad internationella överenskommelser. Behandling av personuppgifter i det syftet ryms också under paragrafen.

I *andra stycket* öppnas en möjlighet att också behandla vissa andra internationella ärenden som ska handläggas av polisen. Uppgifter får i dessa fall behandlas även om det inte är fråga om ett ärende som ingår i polisens brottsbekämpande verksamhet, t.ex. uppgifter om försvinnanden i utlandet.

Gallring

22 § Personuppgifter i det internationella registret ska gallras senast tre år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Paragrafen reglerar gallring av personuppgifter i det internationella registret. Frågan har behandlats i avsnitt 15.5.

Enligt *första stycket* ska personuppgifter gallras senast tre år efter utgången av det kalenderår då ärendet avslutades. Det generella kravet på att uppgifter ska gallras när de inte längre behövs i verksamheten gäller dock även för uppgifter i det internationella registret.

Av *andra stycket* följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att uppgifter, trots vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

5 kap. Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

Ändamål

1 § Personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

a) brott mot rikets säkerhet,

b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,

c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, eller

d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

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

3. fullgöra uppgifter i samband med personskydd,

4. fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627),
5. fullgöra de förpliktelser som följer av internationella åtaganden, eller
6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

Paragrafen anger de primära ändamål för vilka personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet. Avgränsningen av dessa behandlas i avsnitt 16.3.2. I likhet med vad som gäller för övriga polisen får personuppgifter även behandlas för planering, uppföljning och utvärdering av verksamheten. Personuppgifter som behandlas med stöd av 1 § får också behandlas för de sekundära ändamål som anges i 2 § eller för diarieföring m.m. enligt 3 §. Vidare får personuppgifter behandlas för ett nytt ändamål, om det nya ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in. I 4 § anges att vissa bestämmelser i 2 kap. ska tillämpas i Säkerhetspolisens verksamhet. Av hänvisningen i 2 kap. 2 § första stycket punkten 3 till 9 § första stycket d personuppgiftslagen (1998:204) följer att ramarna för sådan vidarebehandling sätts av den s.k. finalitetsprincipen.

Av hänvisningen i 2 kap. 2 § till 8 § personuppgiftslagen följer att behandling av personuppgifter även får ske i den mån den är nödvändig för att Säkerhetspolisen ska kunna fullgöra sina skyldigheter enligt 2 kap. tryckfrihetsförordningen.

En grundläggande förutsättning för att behandling ska vara tillåten är att behandlingen behövs för den verksamhet som anges i paragrafen. Det innebär att det ska finnas ett konkret behov av att utföra behandlingen och att detta behov svarar mot något av de ändamål som anges i paragrafen.

I sammanhanget kan också erinras om att vissa av kapitlets bestämmelser ska tillämpas på juridiska personer, se 1 kap. 3 §.

I *punkten 1 a* nämns en av Säkerhetspolisens huvuduppgifter, att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som rör brott mot rikets säkerhet. Vidare räknas vissa andra typer av brott upp som Säkerhetspolisen har huvudansvar för att bekämpa, nämligen terroristbrott och brott som avser finansiering av terrorism (*punkterna 1 b och 1 c*). Med brott mot rikets säkerhet brukar främst avses brott mot bestämmelserna i 18 och 19 kap. brottsbalken samt brott mot vissa bestämmelser i 13 kap. brottsbalken (bl.a. 13 kap. 1, 2, 3, 5 a och 5 b §§), beroende på syftet med brottet. Med terroristbrott avses framför allt brott mot lagen (2003:148) om straff för terroristbrott och lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall. Enligt föreskrifter som Rikspolisstyrelsen har meddelat ska förundersökningar avseende yttrandefrihetsbrott och tryckfrihetsbrott med rasistiskt eller främlingsfientligt motiv alltid handhas av Säkerhetspolisen eller under medverkan av Säkerhetspolisen i de fall där Justitiekanslern är ensam åklagare (RPSFS 1999:10, FAP 403–3). Säkerhetspolisen får enligt *punkten 1 d* behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka sådana brott.

Under ändamålet förebygga, förhindra eller upptäcka brottslig verksamhet faller bl.a. Säkerhetspolisens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag. Insamling av uppgifter rörande verksamheter, sammanslutningar

och annat som kan utvecklas till konkreta hot mot det svenska samhällsskicket eller mot enskilda personer i statsledningen är ett annat exempel. Vidare hör spaning i syfte att uppdaga sådan brottslig verksamhet som Säkerhetspolisen bekämpar hit. När uttrycket brottslig verksamhet används i lagen i övrigt syftar det på verksamhet av viss konkretion. Detsamma gäller i detta sammanhang, även om det här rör sig om helt andra typer av företeelser och verksamheter där anknytningen till urskiljbara brott ofta inte är lika tydlig. Säkerhetspolisens underrättelseverksamhet har således en bredare inriktning än motsvarande verksamhet hos den övriga polisen, eftersom den senare är tydligare inriktad på vissa brottstyper eller brottsliga företeelser. Även i Säkerhetspolisens underrättelseverksamhet krävs det emellertid att ändamålet med insamlingen eller bearbetningen av personuppgifter kan preciseras. Det kan t.ex. vara fråga om att en främmande stat misstänks bedriva underrättelseverksamhet av visst slag, utan att några konkreta brott kan urskiljas. Det kan också röra sig om företeelser i det svenska samhället som kan komma att utvecklas till brott mot bestämmelser i 18 eller 19 kap. brottsbalken.

Handläggningen av tvångsmedelsfrågor enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott inryms också.

Under det nu aktuella ändamålet faller även viss behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken, om syftet är att använda överskottsinformationen för att förhindra brott som anges i punkten 1. Övrig användning av överskottsinformation faller, på samma sätt som för polisen i övrigt, under punkten 2.

Punkten 2 behandlar utredning och beivrande av brott som ligger inom Säkerhetspolisens primära verksamhetsområde, dvs. sådana brott som anges i punkten 1. Vidare omfattas utredning och beivrande av brott i de fall där Säkerhetspolisen har hand om eller är delaktig i utredningen efter särskilt beslut. Vad som avses med uttrycket ”utreda eller beivra brott” utvecklas närmare i kommentaren till 2 kap. 7 §. Som framhållits där ska det vara fråga om konkreta brott. Under denna punkt faller bl.a. det biträde som Säkerhetspolisen ger åklagare i förundersökningar, inkluderande hanteringen av hemliga tvångsmedel. Även spaning under förundersökning hör hit, liksom användning av överskottsinformation för att utreda brott.

Det ändamål som anges i *punkten 3* täcker den personuppgiftsbehandling som behövs för att Säkerhetspolisen ska kunna fullgöra sina uppgifter att skydda bl.a. den centrala statsledningen. 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 samt uppgifter rörande personer som kan utgöra hot mot den skyddade personen. Det är dock enbart uppgifter som behövs för att skyddsuppgiften ska kunna fullgöras som får behandlas. Punkten täcker dessutom behandlingen av personuppgifter för själva bevaknings- och säkerhetsarbetet, exempelvis uppgifter om vem som fullgör bevakningsuppgiften vid ett visst tillfälle.

Eftersom personskydd ytterst syftar till att förebygga brott mot den skyddade personen, kan personuppgiftsbehandling för detta syfte till viss del falla under punkten 1. Säkerhetspolisens uppgift att förebygga brott omfattar emellertid bara vissa typer av brott. Dessutom är långt ifrån alla brott mot person straffbara på planeringsstadiet. Punkten 3 ger tillsam-

mans med punkten 1 stöd för den personuppgiftsbehandling som behövs för Säkerhetspolisens personskydd.

Säkerhetspolisens personuppgiftsbehandling för att fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627) täcks av *punkten 4*. I dessa uppgifter ingår bl.a. registerkontroll och utlämnande av uppgifter med anledning av sådan kontroll.

I *punkten 5* regleras den personuppgiftsbehandling som krävs för att Säkerhetspolisen ska kunna fullgöra internationella åtaganden. Till dessa hör bl.a. att skydda vissa företrädare för utländska stater som besöker Sverige, bl.a. statsöverhuvuden och regeringsföreträdare. I den mån skyddet av dessa inte faller in under punkten 3, t.ex. därför att skyddet i huvudsak fullgörs av utländsk säkerhetspersonal, regleras det i denna punkt.

Säkerhetspolisen lämnar, i likhet med den övriga polisen, i viss utsträckning andra länder rättslig hjälp i brottsutredningar. Det kan exempelvis gälla hjälp med att hålla förhör med en viss person eller att verkställa en tvångsåtgärd. Denna punkt omfattar även den behandling av personuppgifter som behövs i sådana sammanhang.

Under denna punkt faller också Säkerhetspolisens regelbundna informations- och erfarenhetsutbyte med motsvarande myndigheter i andra länder, i den mån detta utbyte grundar sig på ett internationellt åtagande. Om informationsutbytet äger rum enbart i svenskt intresse faller det normalt under någon av de tidigare punkterna. Däremot hör sådant informationsutbyte som enbart gagnar den utländska myndigheten, t.ex. uppgift om brott i en annan stat, hemma under denna punkt.

Punkten 6 tar sikte på Säkerhetspolisens personuppgiftsbehandling när myndigheten lämnar tekniskt biträde till andra brottsbekämpande myndigheter. Sådant biträde kan t.ex. bestå i hjälp med användning av särskild spaningsutrustning. Den vanligaste formen av biträde är dock vid verkställighet av beslut om hemliga tvångsmedel, t.ex. beslut om hemlig teleavlyssning eller hemlig teleövervakning. Punkten täcker dels den behandling av personuppgifter som krävs för att Säkerhetspolisen ska kunna vidarebefordra beslut av domstol eller åklagare i frågor angående dessa tvångsmedel till vederbörande operatör, dels den behandling i form av lagring som sker hos Säkerhetspolisen när operatörerna överför uppgifter dit i enlighet med beslutet. Vidare täcks Säkerhetspolisens biträde vid verkställighet av andra hemliga tvångsmedel, i den mån sådant biträde kräver personuppgiftsbehandling. Så kan t.ex. vara fallet om biträdet rör hemlig rumsavlyssning och Säkerhetspolisen lagrar upptagningarna.

2 § Personuppgifter som behandlas enligt 1 §, får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. en myndighets verksamhet, om tillhandahållandet görs i syfte att samverka mot brott,
3. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller
4. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation.

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

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 1 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter.

Paragrafen reglerar de sekundära ändamål för vilka Säkerhetspolisen får behandla personuppgifter. Skälen för den valda regleringen har redovisats i avsnitt 16.3.3. Behandlingen enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling enligt 1 §. Det är således inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem med stöd av denna paragraf.

Det förhållandet att uppgifterna får behandlas påverkar inte heller de bestämmelser som gäller om sekretess. Bestämmelserna i offentlighets- och sekretesslagen (2009:400) om sekretess mellan myndigheter ska därför beaktas på vanligt sätt i den utsträckning det inte finns särskilda sekretessbrytande regler. Uppgifter kan alltså inte lämnas ut om sekretess hindrar det. I 4 § 6 hänvisas till regler i 2 kap. som är sekretessbrytande.

Paragrafen motsvarar i stora delar regleringen för polisen i övrigt (se 2 kap. 8 §). En skillnad är dock att Säkerhetspolisen inte får behandla uppgifter för att lämna information till den övriga polisen i syfte att denna ska användas för annat ändamål än brottsbekämpning. Däremot öppnas möjlighet till informationsutbyte med Försvarsmaktens underrättelseverksamhet, vilket inte har någon motsvarighet i polisverksamheten i övrigt.

Första stycket reglerar Säkerhetspolisens möjlighet att behandla uppgifter för att kunna lämna dem till bl.a. en annan brottsbekämpande myndighet. Enligt *punkten 1* får Säkerhetspolisen, vars brottsbekämpning rör ett relativt begränsat område, utföra den behandling som krävs för att vidarebefordra bl.a. uppgifter om brott eller brottslig verksamhet som Säkerhetspolisen upptäcker men saknar behörighet att handlägga. Som exempel kan nämnas att det vid hemlig teleavlyssning visar sig att någon av de avlyssnade personerna planerar att begå ett rån eller att det kommer fram uppgifter om en leverans av narkotika. Sådana uppgifter måste kunna bli föremål för den behandling som krävs för att Säkerhetspolisen ska kunna lämna över dem till den enhet inom polisen eller en annan brottsbekämpande myndighet som har till uppgift att ingripa mot brottet (Tullverket i exemplet med narkotikan om det rör sig om smuggling). Säkerhetspolisen kan också ha behov av att till en annan enhet inom polisen lämna sådana uppgifter som har samband med personskyddet, t.ex. uppgifter om planerade eller begångna brott som inte är av den arten att de utreds av Säkerhetspolisen.

Punkten 2 öppnar en möjlighet för Säkerhetspolisen att behandla uppgifter för att lämna dem till en myndighet i syfte att samverka mot brott. En motsvarande bestämmelse finns för den övriga polisen i 2 kap. 8 § första stycket 6 b. I första hand tillgodoser punkten behovet av informationsutbyte med andra myndigheter än brottsbekämpande, eftersom punkten 1 i huvudsak täcker det behovet. Uppgiftslämnande till myndig-

het som anges i punkten 3 kan ske med stöd av denna punkt om syftet är att samverka mot brott.

Enligt *punkten 3* får Säkerhetspolisen även behandla uppgifter för att kunna lämna dem till Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Syftet med bestämmelsen är främst att Säkerhetspolisen ska kunna behandla personuppgifter som den anser kan vara värdefulla för Försvarsmakten och därför vill vidarebefordra dit. Möjligheterna till sådan behandling begränsas genom kravet på att det ska finnas särskilda skäl att tillhandahålla informationen. Som exempel på särskilda skäl kan nämnas att det under en förundersökning som Säkerhetspolisen bedriver kommer fram information som kan vara mycket viktig för Försvarsmakten i dess underrättelseverksamhet. Ett annat exempel kan vara att Säkerhetspolisen i sin brottsbekämpning noterar svagheter eller brister i skyddet för Försvarsmaktens anläggningar som skulle kunna få allvarliga konsekvenser. Om uppgifterna lämnas i syfte att samverka mot brott faller behandlingen inte under denna punkt utan under punkten 2.

I *punkten 4* regleras möjligheten att behandla personuppgifter för att lämna uppgifter till en utländsk myndighet eller mellanfolklig organisation. Enligt denna punkt kan information, som ändå behandlas enligt 1 §, också behandlas för att tillhandahålla information som är nödvändig för den brottsbekämpande verksamheten vid en utländsk myndighet eller en mellanfolklig organisation. Exempel på uppgifter som kan lämnas ut med stöd av denna punkt är uppgifter om brott, brottsmisstankar och misstänkt brottslig verksamhet men också uppgifter som härrör från personskyddet, t.ex. aktuella hotbilder, om det behövs för att den utländska myndigheten ska kunna skydda en svensk företrädare för den centrala statsledningen som gör ett officiellt besök i det andra landet. I 2 kap. 15 §, som enligt 4 § 6 ska tillämpas även av Säkerhetspolisen, finns en regel om utlämnande av uppgifter till utländsk myndighet eller mellanfolklig organisation. Denna regel är sekretessbrytande.

Andra och *tredje styckena* motsvarar 2 kap. 8 § andra och tredje styckena. I fråga om innebörden hänvisas till kommentaren till den paragrafen.

3 § Personuppgifter får behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Paragrafen innebär att personuppgifter alltid får behandlas om behandlingen är nödvändig för diarieföring eller, om uppgifterna har lämnats i en anmälan eller liknande, för handläggningen. För övriga polisen finns en motsvarande regel i 2 kap. 9 §. För en närmare beskrivning av innebörden av bestämmelserna hänvisas till kommentaren till den paragrafen.

Tillämpliga bestämmelser i 2 kap.

4 § Följande bestämmelser i 2 kap. ska tillämpas vid behandling av personuppgifter hos Säkerhetspolisen:

1. 1 och 2 §§ om förhållandet till personuppgiftslagen (1998:204),

2. 3 § om definition av DNA-analys, DNA-profil och fingeravtryck,
3. 6 § om tillsyn,
4. 10 § om behandling av känsliga personuppgifter,
5. 11 § om tillgången till personuppgifter,
6. 14, 15 och 19 §§ om utlämnande av personuppgifter och uppgiftsskyldighet, och
7. 20 och 21 §§ om elektroniskt utlämnande av personuppgifter.

I paragrafen anges vilka av bestämmelserna i 2 kap. som ska tillämpas på den behandling som utförs av Säkerhetspolisen. Frågan har behandlats i avsnitt 16.2.2.

Av *punkten 1* följer att förevarande lag ska tillämpas i stället för personuppgiftslagen (1998:204), om inte annat framgår av 2 kap. 2 §. I sistnämnda paragraf räknas upp vilka regler i personuppgiftslagen som ska tillämpas. Urvalet av bestämmelser beskrivs närmare i kommentaren till den paragrafen.

Hänvisningen i *punkten 2* innebär att definitionerna i 2 kap. 3 § ska tillämpas även i Säkerhetspolisens verksamhet.

Genom hänvisningen i *punkten 3* till 2 kap. 6 § tydliggörs att vad som sägs där om tillsyn även gäller för Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten.

Hänvisningen i *punkten 4* till 2 kap. 10 § innebär att Säkerhetspolisen ska tillämpa samma grundläggande regler vid behandling av känsliga personuppgifter som polisen i övrigt.

Vidare ska enligt *punkten 5* bestämmelsen i 2 kap. 11 § tillämpas på Säkerhetspolisen. Den innebär att varje persons tillgång till personuppgifter ska begränsas till vad han eller hon behöver för att fullgöra sina arbetsuppgifter. Som framgår av kommentaren till den paragrafen avses inte bara tillgång genom direktåtkomst utan även annan tillgång till uppgifter.

Enligt *punkten 6* ska de sekretessbrytande bestämmelserna i 2 kap. 14 § om utlämnande av statistikuppgifter, 15 § om utlämnande av uppgifter till utländska myndigheter och mellanfolkliga organisationer och 19 § om möjlighet att meddela föreskrifter, tillämpas också på Säkerhetspolisens brottsbekämpande verksamhet.

Slutligen ska enligt *punkten 7* bestämmelserna i 2 kap. 20 och 21 §§ om elektroniskt utlämnande tillämpas även av Säkerhetspolisen.

Personuppgiftsansvar

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

Säkerhetspolisen ska utse ett eller flera personuppgiftsombud. Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Paragrafen har behandlats i avsnitt 16.2.2.

Första stycket innehåller en bestämmelse om personuppgiftsansvar. Bestämmelsen innebär att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför.

I *andra stycket* föreskrivs att Säkerhetspolisen, på motsvarande sätt som Rikspolisstyrelsen och polismyndigheterna, ska utse ett eller flera personuppgiftsombud samt anmäla till tillsynsmyndigheten, dvs. Datainspektionen, när ett personuppgiftsombud utses eller entledigas.

Motsvarande bestämmelser för polisens övriga brottsbekämpande verksamhet finns i 2 kap. 4 och 5 §§.

Bevarande och gallring

6 § Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av ändamålen i 1–3 §§.

I 7 och 12–14 §§ anges hur länge uppgifter som behandlas automatiserat längst får bevaras.

Regeringen meddelar föreskrifter om digital arkivering.

Paragrafen, som har behandlats i avsnitt 16.2.2, innehåller en generell bestämmelse om längsta tid för bevarande av uppgifter och hänvisar till de övriga bestämmelser i kapitlet som reglerar bevarande och gallring.

Av *första stycket* framgår att personuppgifter aldrig får bevaras längre än vad som behövs för något eller några av de ändamål för Säkerhetspolisens personuppgiftsbehandling som anges i lagen. Motsvarande regel finns i 2 kap. 12 § för polisen i övrigt och i kommentaren till den paragrafen utvecklas den närmare innebörden av bestämmelsen.

Andra stycket är en informationsbestämmelse som syftar till att underlätta för tillämparen genom att ange samtliga bestämmelser om bevarande och gallring som är tillämpliga på Säkerhetspolisens personuppgiftsbehandling.

I *tredje stycket* finns en upplysning om att regeringen kan meddela föreskrifter om digital arkivering, i likhet med vad som gäller för övriga polisen. Syftet med sådana föreskrifter kan vara att förhindra att digitalt arkiverade uppgifter fortsätter att behandlas på samma sätt som tidigare i Säkerhetspolisens brottsbekämpande verksamheten, trots att bevarandet inte längre sker för verksamhetsändamål utan för arkivändamål.

7 § Personuppgifter som behandlas automatiserat hos Säkerhetspolisen och som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Paragrafen innehåller gallringsregler för sådana personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga. För gemensamt tillgängliga uppgifter gäller andra gallringsregler i 12 och 13 §§. Skälen för den valda lösningen har redovisats i avsnitt 16.2.2. och 16.4.4.

Enligt *första stycket* ska personuppgifter som behandlas automatiserat i ett ärende gallras senast ett år efter det att ärendet avslutades, medan

uppgifter som inte hör till något ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången. En motsvarande bestämmelse för polisens övriga brottsbekämpande verksamhet finns i 2 kap. 13 § första stycket. Vad som avses med ett ärende och med gallring utvecklas närmare i kommentaren till den paragrafen.

I *andra stycket* görs undantag för uppgifter i ärenden om utredning eller beivrande av brott. Detta motsvarar regleringen i 2 kap. 13 § andra stycket. Innebörden av bestämmelsen kommenteras under den paragrafen.

Av *tredje stycket* följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att personuppgifter, trots vad som sägs i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande bestämmelse finns i 2 kap. 13 § tredje stycket.

Behandling av gemensamt tillgängliga uppgifter

Gemensamt tillgängliga uppgifter

8 § Om det behövs för de ändamål som anges i 1 §, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet. Detta gäller dock inte DNA-profiler. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Bestämmelserna i 9–13 §§ gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Bestämmelserna gäller dock inte när personuppgifter behandlas med stöd av 3 §.

Paragrafen reglerar vilka uppgifter som får göras gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet. Frågan har berörts i avsnitt 16.4.1. Vad som avses med gemensamt tillgängliga uppgifter har behandlats i avsnitt 9 och i kommentaren till 3 kap. 1 §.

I *första stycket* slås fast att personuppgifter får göras gemensamt tillgängliga om det behövs för de primära ändamål för vilka Säkerhetspolisen får behandla uppgifter. DNA-profiler får dock aldrig göras gemensamt tillgängliga. Sistnämnda bestämmelse motsvarar vad som gäller för polisen i övrigt, se 3 kap. 2 § andra stycket. I kommentaren till 2 kap. 3 § redovisas vad som avses med DNA-profil.

Av *andra stycket* framgår att bestämmelserna i 9–13 §§ ska tillämpas i de fall där personuppgifter har gjorts gemensamt tillgängliga. Det innebär bl.a. att andra gallringsfrister gäller och att det genom en särskild upplysning eller på något annat sätt ska framgå för vilket närmare ändamål en personuppgift behandlas. Bestämmelserna i 9–13 §§ gäller dock inte för sådan behandling av uppgifter som sker med stöd av bestämmelserna i 3 §. I kommentaren till 2 kap. 9 § redogörs närmare för vilken personuppgiftsbehandling som får ske vid diarieföring eller i fråga om uppgifter som lämnas till polisen i anmälan eller liknande handling.

Särskilda upplysningar

9 § Vid behandling enligt 8 § ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas.

I paragrafen, som delvis motsvarar 3 kap. 3 §, ställs krav på att det närmare ändamål för vilket en personuppgift behandlas ska framgå. Frågan har behandlats i avsnitt 16.4.2.

Om uppgifter samlas in för ett visst ändamål, men senare kommer att användas för ett annat ändamål, måste en upplysning om det nya ändamålet lämnas vid den senare behandlingen. Så blir t.ex. fallet om uppgifter, som har framkommit i ett underrättelseprojekt, senare utnyttjas i personskyddet eller om uppgifter från en förundersökning tillförs ett underrättelseprojekt.

I de fall där det framgår av omständigheterna för vilket ändamål en uppgift behandlas krävs inte någon särskild upplysning. Uppgifter i t.ex. en förundersökning, i en annan utredning enligt 23 kap. rättegångsbalken eller i ett avgränsat underrättelseprojekt behöver därför normalt inte förses med någon särskild upplysning. Även vid behandling av personuppgifter i bild- eller ljudupptagningar eller i löpande text brukar det som regel framgå av sammanhanget varför uppgifterna behandlas. Tanken är således inte att varje enskild uppgift alltid ska förses med en särskild upplysning. Det krävs dock att upptagningen, textfilen eller textavsnittet förses med en upplysning om varifrån den härrör och varför den behandlas, om detta inte framgår på något annat sätt.

10 § Om uppgifter, som behandlas enligt 8 §, 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.

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. Sådan upplysning behöver dock inte lämnas, om det på grund av särskilda omständigheter är onödigt. Någon upplysning 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 och analysen befinner sig i ett inledande skede.

I paragrafen föreskrivs att det vid behandling av uppgifter som har gjorts gemensamt tillgängliga ska framgå om en uppgift avser en person som inte är misstänkt. Vidare föreskrivs att viss information ska värderas och förses med en upplysning om resultatet av värderingen. Skälen för detta har angetts i avsnitt 16.4.2. Bestämmelserna motsvarar i allt väsentligt vad som gäller för polisens övriga brottsbekämpande verksamhet enligt 3 kap. 4 §.

Uttrycket ”uppgifter som direkt kan hänföras till en person” innebär att paragrafen bara är tillämplig på direkta personuppgifter. Om den person som en sådan uppgift gäller inte är misstänkt vare sig för något brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska detta enligt *första stycket* framgå genom en särskild upplysning eller på något annat sätt. Som påpekas i kommentaren till 3 kap. 4 § första stycket inträder skyldigheten bara om det inte alls finns någon misstanke.

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med brottslig verksamhet förses med en upplysning om uppgifts-

lämnarens trovärdighet och uppgifternas riktighet i sak. Motsvarande bestämmelse gäller för övriga polisen. För en närmare beskrivning av innebörden av bestämmelsen hänvisas till kommentaren till 3 kap. 4 § andra stycket.

Uppgift om uppgiftslämnares trovärdighet och uppgifternas riktighet i sak behöver, liksom enligt 3 kap. 4 §, inte lämnas om det på grund av särskilda omständigheter är onödigt. Vad som avses med detta kommenteras under den paragrafen.

Vidare har undantag gjorts för uppgifter i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt utpekade tjänstemän har tillgång till och där bearbetningen och analysen befinner sig i ett första, inledande skede. Detta undantag saknar motsvarighet i 3 kap. 4 §. Med inledande skede avses här den tid efter det att en uppgift har tillförts en sådan uppgiftssamling och under vilken det inte är möjligt att bedöma om uppgiften har betydelse för analysarbetet eller kan avföras som ointressant. Undantaget innebär att personuppgifterna under detta skede, som ska vara en kortare tid, inte behöver kompletteras med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Om analysarbetet däremot leder vidare t.ex. till en fördjupad analys av vissa personers kontakter eller förehavanden eller till en förundersökning, måste personuppgifterna kompletteras med särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Sökning

11 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som anges i 1 §.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om sökning i gemensamt tillgängliga uppgifter.

Paragrafen reglerar möjligheterna att använda känsliga personuppgifter som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Skälen för den valda lösningen har redovisats i avsnitt 16.4.3. Bestämmelsen gäller bara för uppgifter som har gjorts gemensamt tillgängliga.

I motsats till vad som gäller för polisen i övrigt får Säkerhetspolisen, enligt *första stycket*, i begränsad utsträckning använda känsliga personuppgifter som sökbegrepp. Uppgifter som rör politiska åsikter kan ibland vara av intresse, eftersom det ingår i Säkerhetspolisens uppgifter att kartlägga sådan politisk verksamhet som kan komma att hota vitala samhällsfunktioner. Vid underrättelseverksamhet eller utredning av terroristbrott kan andra känsliga uppgifter vara väsentliga. Kravet på att det ska vara absolut nödvändigt från verksamhetssynpunkt att använda ett sådant sökbegrepp gör dock att utrymmet för sådana sökningar är begränsat och att rutinmässiga sökningar på känsliga uppgifter inte är tillåtna.

I *andra stycket* görs klart att brottsrubriceringar och uppgifter som beskriver en persons utseende får användas som sökbegrepp. En motsvarande bestämmelse finns i 3 kap. 5 § andra stycket för den övriga polisen. I fråga om innebörden hänvisas till kommentaren till den paragrafen.

I *tredje stycket* informeras om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om sökning i gemensamt tillgängliga uppgifter i Säkerhetspolisens brottsbekämpande verksamhet.

Bevarande och gallring

12 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en sådan uppgiftssamling som avses i 10 § andra stycket 1 ska dock 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 än vad som anges i första och andra styckena, om uppgifterna fortfarande behövs för det ändamål som de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i andra stycket, senast vid utgången av det tredje kalenderåret efter beslutet.

Paragrafen innehåller bestämmelser som, tillsammans med 13 §, reglerar bevarande och gallring av gemensamt tillgängliga uppgifter. Bestämmelserna kompletterar den allmänna bestämmelsen i 6 §. För gallring av uppgifter som inte har gjorts gemensamt tillgängliga tillämpas 7 §. Vad som avses med gallring redovisas i kommentaren till 2 kap. 13 § och 3 kap. 9 §. Frågor om bevarande och gallring vid Säkerhetspolisens personuppgiftsbehandling har behandlats i avsnitt 16.2.2 och 16.4.4.

Skilda gallringsfrister gäller för olika typer av uppgifter. Huvudregeln, som anges i *första stycket,* är att personuppgifter som har gjorts gemensamt tillgängliga inom Säkerhetspolisen ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen beträffande den aktuella personen gjordes. Detta motsvarar vad som enligt 35 § polisdatalagen (1998:622) gäller för gallring av personuppgifter i SÄPO-registret.

Enligt *andra stycket* ska uppgifter i sådana särskilda uppgiftssamlingar som avses i 10 § andra stycket 1 gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om nya uppgifter om personen samlas in, förlängs alltså gallringsfristen. Detta gäller oavsett om uppgifterna har samband med den först aktuella brottsliga verksamheten eller samlas in av annat skäl.

I *tredje stycket* öppnas en möjlighet för Säkerhetspolisen att, om det finns särskilda skäl, genom ett särskilt beslut i det enskilda fallet förlänga gallringsfristen. Detta förutsätter att personuppgifterna fortfarande behövs för de ändamål för vilka de behandlas. Ett beslut av detta slag ska fattas innan gallringsfristen har löpt ut. Har Säkerhetspolisen meddelat ett beslut om fortsatt bevarande, ska uppgifterna som huvudregel gallras – eller frågan om bevarande prövas på nytt – senast vid utgången av det

tionde året efter beslutet. Uppgifter som avses i andra stycket ska dock gallras, eller beslutet omprövas, senast vid utgången av det tredje kalenderåret efter beslutet.

13 § Bestämmelserna i 12 § gäller inte personuppgifter i ärenden om utredning eller beivrande av brott. I fråga om behandling av sådana personuppgifter ska i stället 3 kap. 9–13 §§ tillämpas.

Bakgrunden till paragrafen har tecknats i avsnitt 16.4.4. I paragrafen görs undantag från gallringsbestämmelserna i 12 § för personuppgifter i ärenden om utredning eller beivrande av brott. I stället ska bestämmelserna i 3 kap. 9–13 §§ tillämpas, dvs. de bestämmelser som gäller för polisens övriga brottsbekämpande verksamhet. Uppgifter som har hämtats från exempelvis en förundersökning för att behandlas för ett nytt ändamål ska dock gallras enligt de frister som gäller för det nya ändamålet, t.ex. personskydd.

14 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 12 §, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Av paragrafen, som har behandlats i avsnitt 16.4.4, följer att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela föreskrifter om att personuppgifter, trots vad som sägs i 12 §, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Övergångsbestämmelser

Övergångsbestämmelserna har behandlats i avsnitt 18.

22.2 Förslaget till lag om polisens allmänna spaningsregister

Allmänt spaningsregister

1 § Rikspolisstyrelsen får med hjälp av automatiserad behandling föra ett allmänt spaningsregister.

Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Enligt paragrafens *första stycke* får Rikspolisstyrelsen föra ett allmänt spaningsregister. Registret, som ska vara nationellt, får föras med hjälp av automatiserad behandling. Vilken behandling av personuppgifter som är tillåten i övrigt i polisens brottsbekämpande verksamhet styrs framför allt av lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Motiveringen till särregleringen av det allmänna spaningsregistret har redovisats i avsnitt 19.1.

I *andra stycket* slås fast att Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av uppgifter i registret.

Förhållandet till personuppgiftslagen

2 § Personuppgiftslagen (1998:204) gäller vid behandling av personuppgifter i det allmänna spaningsregistret, om inte annat följer av denna lag eller av föreskrifter som har meddelats i anslutning till denna lag.

I paragrafen regleras lagens förhållande till personuppgiftslagen (1998:204). Av paragrafen framgår att personuppgiftslagen ska tillämpas när personuppgifter behandlas i det allmänna spaningsregistret, om inte annat sägs i lagen om registret eller i föreskrifter som har meddelats i anslutning till den lagen. Lagen innehåller endast de särbestämmelser som det har bedömts finnas behov av. I övrigt ska personuppgiftslagen tillämpas. I förtydligande syfte har i 4 § uttryckligen hänvisats till en viss bestämmelse i personuppgiftslagen och i 26 § har två andra bestämmelser i den lagen gjorts tillämpliga. Lagens förhållande till personuppgiftslagen har behandlats i avsnitt 19.2.

Ändamål

3 § Det allmänna spaningsregistret ska ha till ändamål att utgöra underlag för systematisering av vissa personuppgifter som framkommit i polisens brottsbekämpande verksamhet. Registret får föras för att underlätta tillgången till sådan information som behövs i polisens spaningsverksamhet.

I paragrafen anges det primära ändamålet med registret, vilket är att utgöra underlag för systematisering av vissa personuppgifter i polisens brottsbekämpande verksamhet. Registret är ett verksamhetsstöd särskilt anpassat för polisens spaningsverksamhet. Registret får föras för att underlätta tillgången till information som behövs i sådan verksamhet. Detta återspeglas i 5–9 §§, som reglerar vilka personuppgifter som får behandlas och det närmare innehållet i registret. Med polisens brottsbekämpande verksamhet avses detsamma som i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Regleringen av ändamålen har behandlats i avsnitt 19.3.

Med spaningsverksamhet avses såväl den spaning som äger rum under en förundersökning (23 kap. 2 § rättegångsbalken) som spaning som polisen bedriver inom ramen för arbetet med att förebygga, förhindra och upptäcka brott. Även spaning efter personer som är efterlysta såsom anhållna eller häktade i sin frånvaro hör hit. Sådan spaning som inte hör till den brottsbekämpande verksamheten faller däremot utanför paragrafens tillämpningsområde. Att uppgifter i registret under vissa förutsättningar får tillhandahållas annan verksamhet framgår av 4 §.

Av andra meningen följer att endast sådana uppgifter som behövs i spaningsverksamheten får behandlas. Uppgifter som härrör från andra register eller från uppgiftssamlingar som redan är tillgängliga för flertalet polismän finns det i allmänhet inget behov av att föra in i registret. Som exempel kan nämnas att det sällan torde vara nödvändigt att föra över uppgifter från belastningsregistret eller misstankeregistret till det allmänna spaningsregistret, eftersom hela polisväsendet ändå har tillgång till dessa uppgifter. Det finns inte heller något behov av att notera att det i andra register finns fingeravtryck eller DNA-profil av en misstänkt.

4 § Personuppgifter i registret får behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,
3. sådan verksamhet hos polisen som avser handräckningsuppdrag, eller
4. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen.

Personuppgifter får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. I övrigt gäller 9 § första stycket d personuppgiftslagen (1998:204).

Paragrafen, som i stora delar motsvarar 2 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, anger de sekundära ändamål för vilka personuppgifter får behandlas i registret. Frågan har behandlats i avsnitt 19.3.

Behandling av personuppgifter enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling med stöd av 3 §. Det är alltså inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem enligt denna paragraf. Utgångspunkten är att de angivna sekundära ändamålen i allt väsentligt ska täcka in det utlämnande av uppgifter som kan komma i fråga. För att behandling för andra ändamål än de i paragrafen uppräknade ska vara tillåten krävs att den inte kan anses vara oförenlig med insamlingsändamålet (finalitetsprincipen). Det förhållandet att uppgifter i vissa fall får behandlas för utlämnande av information påverkar inte de bestämmelser som gäller om sekretess. Bestämmelserna i offentlighets- och sekretesslagen (2009:400) om sekretess mellan myndigheter, liksom bestämmelser i andra författningar som bryter sekretess, ska således beaktas på vanligt sätt. I kommentaren till 16–18 §§ behandlas de särskilda sekretessbrytande bestämmelserna i denna lag.

Enligt *första stycket punkten 1* får personuppgifter som behandlas med stöd av 3 § behandlas för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos de uppräknade myndigheterna. Med stöd av bestämmelsen kan uppgifter även tillhandahållas Säkerhetspolisen, som utgör en del av Rikspolisstyrelsen (jfr kommentaren till 2 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet).

Punkten 2 ger möjlighet att behandla personuppgifter som behandlas enligt 3 § för att tillhandahålla en utländsk myndighet eller mellanfolklig organisation den information som behövs i dess brottsbekämpande verksamhet. De utländska myndigheter som avses i punkten 2 är främst polis- och åklagarmyndigheter. Möjligheten att behandla uppgifterna genom att lämna ut dem kan begränsas inte bara av sekretess utan även av reglerna i 33–35 §§ personuppgiftslagen (1998:204), som inskränker möjligheten att överföra uppgifter till tredjeland.

Enligt *punkten 3* får personuppgifter som behandlas med stöd av 3 § även behandlas om det är nödvändigt för att tillhandahålla information som behövs när polisen bistår andra myndigheter med handräckningsuppdrag.

Punkten 4 tar sikte på behandling av personuppgifter för att tillhandahålla uppgifter till sådan polisiär verksamhet som inte är brottsbekämpande och som inte heller avser handräckningsuppdrag. För sådant utlämnande krävs det särskilda skäl. För den närmare innebörden hänvisas till kommentaren till 2 kap. 8 § första stycket 4 lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Enligt *andra stycket* får personuppgifter behandlas om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen, samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till annan. För att tillhandahållande för andra ändamål än de som räknas upp i paragrafen ska vara tillåtet krävs det att behandlingen inte kan anses oförenlig med insamlingsändamålet. Detta tydliggörs genom en hänvisning till den s.k. finalitetsprincipen i 9 § första stycket d personuppgiftslagen.

Innehåll

5 § I registret får uppgifter om en person behandlas, om

1. den som uppgiften avser kan misstänkas för ett brott som inte har enbart böter i straffskalan, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

Bakgrunden till paragrafen har behandlats i avsnitt 19.4.1.

Paragrafen reglerar, tillsammans med 6 och 7 §§, vad som krävs för att uppgifter om en viss fysisk eller juridisk person, eller ett transportmedel eller ett föremål, ska få införas i registret. Det närmare innehållet i registret regleras i 8 och 9 §§.

För att uppgifter om en viss person ska få föras in i registret krävs det enligt huvudregeln att personen misstänks för att ha begått brott. Det är tillräckligt med en misstanke på låg nivå, vilket markeras genom uttrycket ”kan misstänkas”. Uppgifter om personer som enbart misstänks för att utöva eller komma att utöva brottslig verksamhet i någon form får däremot inte föras in i registret.

I stället för att som i tillståndet till det nuvarande spaningsregistret räkna upp vilka brott som får läggas till grund för registrering har valts en generell lösning som bygger på brottets straffskala. Misstanken ska avse brott som inte har enbart böter i straffskalan. Det är emellertid inget som hindrar att Rikspolisstyrelsen inom den ramen närmare anger vilka typer av brott som får ligga till grund för registrering.

Förutom misstanke om ett visst konkret brott krävs det också att behandlingen i registret är av särskild betydelse för polisens spaningsverksamhet. Detta rekvisit motsvarar i princip vad som gäller enligt tillståndet för det allmänna spaningsregistret. Att en uppgift ska ha särskild betydelse för polisens spaningsverksamhet innebär att uppgiften måste vara värdefull antingen i strävandena att förebygga, förhindra eller upptäcka brott eller i verksamheten att utreda brott. Det får med andra ord inte vara en uppgift som polisen både kan ha och mista. Om de krav som ställs i paragrafen är uppfyllda, får uppgifter om personen behandlas.

6 § I registret får uppgifter om en person som inte kan misstänkas för brott behandlas, om

1. uppgiften har samband med en person som har registrerats enligt 5 §, och
2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

I paragrafen regleras i vilken utsträckning uppgifter om andra personer än misstänkta får behandlas i registret. Frågan har tagits upp i avsnitt 19.4.1.

För att registrering ska vara tillåten krävs det dels att uppgiften har samband med en misstänkt som registrerats enligt 5 §, dels att behandlingen har särskild betydelse för polisens spaningsverksamhet. Alla typer av personuppgifter som på något sätt har anknytning till den misstänkta personen kan behandlas. Det kan t.ex. vara uppgifter om hans eller hennes anhöriga, såsom uppgifter om deras innehav av bostad eller transportmedel. Vidare kan uppgifter om andra personer som står den misstänkte nära, eller som den misstänkte tillbringar en stor del av sin tid hos, behandlas. Uppgifter om en person som har funnits i den misstänktes omedelbara närhet när han eller hon har ertappats med att begå brott eller en person hos vilken brottet har begåtts eller mot vilken brott har begåtts kan också falla in under bestämmelsen. Detsamma gäller uppgifter om personer som har setts i den misstänktes sällskap under omständigheter som innebär att personen får anses ha samband med denne. Även uppgifter om någon som tidigare har straffats för brott med direkt anknytning till den misstänktes brottslighet, t.ex. namnet på en hälare som en viss inbrottstjuv ofta vänder sig till, kan falla under bestämmelsen.

Förutom att det krävs att uppgiften ska ha samband med en misstänkt person som är registrerad i det allmänna spaningsregistret krävs det också att behandlingen ska ha särskild betydelse för spaningsverksamheten (jfr 5 § 2). Innebörden av detta är för det första att uppgiften som sådan måste ha relevans för spaningsverksamheten. Det kan uppgiften ha t.ex. om den underlättar eftersökning av den misstänkte, bidrar till upptäckten av brott som han eller hon har begått eller leder till att han eller hon kan knytas som gärningsman till ett visst brott. Uppgifter som uteslutande har betydelse för utredningen av ett brott faller därmed utanför tillämpningsområdet, t.ex. att samla in bevisning mot en viss misstänkt för att styrka ett kommande åtal mot denne.

Det räcker emellertid inte med att en uppgift har relevans för polisens spaningsverksamhet; det krävs också att behandlingen är av särskild betydelse för denna verksamhet. För att exempelvis en uppgift om att två personer sammanträffar med varandra eller att en misstänkt använder en annan persons bil ska anses ha särskild betydelse för spaningsverksamheten krävs det att uppgiften belyser något som – i ett kortare eller längre perspektiv – kan vara till nytta antingen vid ett ingripande mot den misstänkta personen eller vid spaning avseende brott som han eller hon misstänks för.

Särskilda bestämmelser om behandling av uppgifter om personer som inte är misstänkta finns också i 11 och 15 §§.

7 § Utöver de uppgifter som får behandlas enligt 5 och 6 §§, får uppgifter behandlas om en juridisk person eller ett transportmedel eller annat föremål som kan hänföras till en fysisk person, om

1. uppgiften kan antas ha samband med ett brott som inte har enbart böter i straffskalan, och

2. behandlingen är av särskild betydelse för polisens spaningsverksamhet.

I paragrafen regleras behandling av uppgifter som kan hänföras till en person och som har samband med ett brott, men där det inte finns någon person som är misstänkt för brottet. Bakgrunden till paragrafen har tecknats i avsnitt 19.4.2.

Bestämmelsen gör det möjligt att bl.a. registrera uppgifter om juridiska personer och vilken verksamhet de bedriver. Andra exempel på vad som får behandlas är uppgifter om bilar och andra registreringspliktiga fordon. Uppgifter om båtar och fartyg som kan hänföras till en viss person genom fartygsregister eller liknande får också behandlas och likaså uppgifter om flygplan. Ett namn på en båt som är registrerad på en viss person utgör således en sådan personuppgift som får behandlas.

Paragrafen täcker också behandling av uppgifter om andra typer av föremål, om dessa kan knytas till en person på sådant sätt att de utgör personuppgifter. Det kan vara fråga om föremål som det krävs tillstånd att inneha och som kan identifieras genom bl.a. tillverkningsnummer, exempelvis skjutvapen.

I paragrafen ställs det upp två krav som ska vara uppfyllda för att den juridiska personen, transportmedlet eller föremålet ska få registreras. Det ena kravet är att uppgiften kan antas ha samband med ett brott som inte har enbart böter i straffskalan. Uttrycket ”kan antas ha samband med” täcker givetvis även fall där det finns ett påvisat samband. Exempel på uppgifter som kan behandlas enligt paragrafen – om förutsättningarna i övrigt är uppfyllda – är uppgifter om att det förekommer t.ex. omlastning av smuggelgods, tillverkning av narkotika eller förvaring av stöldgods i en lokal som ägs eller disponeras av en juridisk person. Ett annat exempel är en vittnesuppgift som knyter ett visst fordon till en brottsplats. Ytterligare ett exempel är en uppgift om ett fordon som sätts i samband med ett brott därför att fordonet har iakttagits en stund efter brottet på en väg som kan vara en naturlig flyktväg.

Det andra kravet för registrering är att behandlingen är av särskild betydelse för polisens spaningsverksamhet. Det är samma krav som ställs i 5 § första stycket 2 för registrering av en misstänkt person och i 6 § första stycket 2 för behandling av uppgifter om icke misstänkta personer. I fråga om innebörden av begreppet hänvisas till kommentaren till dessa paragrafer.

8 § Registret ska innehålla uppgifter om

1. grunden för att en person registreras som misstänkt enligt 5 § eller att uppgifter om en juridisk person, ett transportmedel eller föremål enligt 7 § förs in i registret och omständigheterna i samband med registreringen,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än sådana som avses i 1 tillförs registret, och
3. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

En upplysning enligt första stycket 3 behöver inte lämnas om det på grund av särskilda omständigheter är onödigt.

I paragrafens *första stycke* slås i tre punkter fast vilka uppgifter som är obligatoriska när det allmänna spaningsregistret tillförs nya uppgifter. Frågan har berörts i avsnitt 19.4.2. Bestämmelserna är tillämpliga både när en fysisk eller juridisk person eller ett transportmedel eller annat

föremål registreras första gången och varje gång det tillförs nya uppgifter om personen i fråga eller om transportmedlet eller föremålet. De två första punkterna, som föreskriver att motivet bakom att uppgifter tillförs registret ska dokumenteras, är alternativa. En av dessa måste alltid tillämpas tillsammans punkten 3.

Punkten 1 är avsedd att användas när uppgifter om en fysisk person registreras på grund av misstanke om brott, dvs. enligt 5 §. Den gäller oavsett om det är fråga om den första registreringen eller att registret tillförs uppgift om en ny brottsmisstanke. Då ska dels grunden för att uppgifterna registreras anges, dels de närmare omständigheterna. Det innebär normalt att det ska anges vilket brott misstanken avser och omständigheterna kring brottet, exempelvis tidpunkten, eventuella medgärningsmän, uppgifter som har betydelse för spaningen etc. Om det uppstår en ny brottsmisstanke ska motsvarande uppgifter anges.

När uppgifter om en juridisk person, ett transportmedel eller annat föremål registreras med stöd av 7 § ska det på motsvarande sätt framgå vilket brott som uppgiften i fråga kan antas ha samband med, skälen för registreringen samt andra uppgifter som är viktiga från spaningssynpunkt.

Punkten 2 reglerar vilka uppgifter som är obligatoriska när man tillför nya uppgifter till de befintliga uppgifterna om en registrerad person, eller uppgifterna om en juridisk person, ett transportmedel eller ett föremål som anges i 7 §. Då ska anges vilka omständigheter eller vilken händelse som gett upphov till att nya uppgifter tillförs. Om en ny uppgift består i exempelvis en iakttagelse av personen på en viss plats eller i visst sällskap, eller en notering om att en registrerad person disponerar ett fordon som ägs av någon annan, ska således detta antecknas. Punkten reglerar även sådan registrering som sker med stöd av 6 §, som ju alltid förutsätter att det redan finns uppgifter registrerade om en misstänkt person.

Slutligen ska enligt *punkten 3* uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak anges. En motsvarande bestämmelse finns i 3 kap. 4 § andra stycket lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Uppgifter ska normalt kunna härledas till en person vars trovärdighet ska värderas. Uppgifter får värderas med utgångspunkt i vad man känner till om personen. I fråga om uppgifter som lämnas av polismän krävs som regel ingen värdering. En bedömning av riktigheten i sak ska alltid göras eftersom en iakttagelse eller bedömning kan vara osäker oberoende av vem den härrör från. När det gäller uppgifternas riktighet i sak får det avgöras av omständigheterna vilka uppgifter som ska anges. Om det är fråga om uppgifter i andra eller tredje hand kan det behövas en mera ingående analys av om uppgifterna har något värde. Det viktiga är att den som får del av uppgiften har möjlighet att med utgångspunkt i upplysningen kunna bedöma hur tillförlitlig uppgiften är.

Enligt *andra stycket* behöver någon upplysning inte lämnas om detta på grund av särskilda omständigheter är onödigt. En motsvarande bestämmelse finns i 3 kap. 4 § andra stycket lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I fråga om innebörden av bestämmelsen hänvisas till kommentaren till den paragrafen.

9 § Registret får, utöver vad som anges i 8 §, innehålla följande uppgifter om en person som har registrerats enligt 5 §:

1. uppgift som är ägnad att identifiera personen, dock inte DNA-profil eller fingeravtryck,
2. uppgift om vistelseadress,
3. uppgift om verkställighet av påföljd för brott,
4. uppgift om att personen är eftersökt i samband med brott,
5. uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
6. uppgift om att personen är föremål för sådan övervakning som avses i 3 kap. 2 § första stycket 2 lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
7. uppgift om anknytning till juridisk person,
8. uppgift om anknytning till andra personer som har registrerats enligt 5 § och som kan antas tillhöra samma gruppering som den registrerade,
9. uppgift om att personen har använt något speciellt tillvägagångssätt, och
10. ärendenummer.

Paragrafen innehåller bestämmelser om vilka uppgifter som får behandlas beträffande den som har antecknats i registret såsom misstänkt. Den tar enbart sikte på uppgifter som rör den registrerade själv. Den allmänna utgångspunkten är att uppgifterna i fråga ska ha särskild betydelse för spaningsverksamheten, eftersom det är det grundläggande ändamålet med behandlingen. Frågan har behandlats i avsnitt 19.4.2.

Enligt *punkten 1* får uppgifter som är ägnade att identifiera personen antecknas. Med detta avses bl.a. uppgifter om namn, födelsetid, personnummer eller annat liknande identitetsnummer, adress, arbetsplats, öknamn, nationalitet, signalementsuppgifter och särskilda fysiska kännetecken samt andra uppgifter som kan bidra till att underlätta identifieringen. Det är dock inte tillåtet att registrera fingeravtryck eller DNA-profiler.

Med *punkten 2,* vistelseadress, avses inte den adress där en person är skriven utan andra adresser där han eller hon vistas. Det kan röra sig om en adress till en anhörig, t.ex. föräldrar, make/maka eller sambo. Det kan också vara fråga om adressen till en eller flera flickvänner eller pojkvänner. Om någon regelbundet besöker eller övernattar i en mc-klubbs lokaler kan detta också anses vara en vistelseadress. En adress där den misstänkte vistas enbart tillfälligt, t.ex. om denne vid något enstaka tillfälle övernattar hos en bekant, kan däremot inte anses utgöra en vistelseadress. Det krävs således en fastare anknytning till adressen i fråga. Uppgifter av det här slaget kan snabbt bli inaktuella och kräver därför särskild vaksamhet. En vistelseadress kan även avse en plats som saknar formell adress, t.ex. en sommarstuga eller jaktstuga.

Enligt *punkten* 3 får uppgifter om verkställighet av påföljd antecknas i registret. Sådana uppgifter kan t.ex. vara att den misstänkte avtjänar fängelsestraff och på vilken kriminalvårdsanstalt denne är intagen. Uppgifter av det slaget har betydelse vid spaningen bl.a. på det sättet att det snabbt går att kontrollera var den misstänkte har befunnit sig vid ett visst tillfälle.

Punkten 4 tar sikte på uppgifter om att personen är eftersökt i samband brott. Det kan t.ex. vara fråga om ett hämtningsbeslut som inte har verkställts eller att personen ska delges stämning eller kallelse till domstol.

Om uppgifterna finns i ett annat register, exempelvis efterlysningsregistret, finns det normalt inget behov av att föra in samma uppgifter i det allmänna spaningsregistret, jfr kommentaren till 2 §.

Uppgifter om att en person tidigare har agerat på sådant sätt att man bör närma sig honom eller henne med försiktighet regleras i *punkten 5*. Enligt den punkten får registret innehålla uppgifter om att personen vid tidigare ingripanden varit beväpnad, våldsam eller visat flyktbenägenhet. Uppgifter av det slaget kan ha stor betydelse för planeringen av polisiära ingripanden.

Registret får enligt *punkten 6* också innehålla uppgift om att en person är föremål för övervakning med stöd av 3 kap. 2 § första stycket 2 lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det möjliggör för polisen att fånga upp iakttagelser om den övervakade personen som görs av andra polismän än de som hanterar övervakningen.

Vidare får enligt *punkten 7* uppgifter om den misstänktes anknytning till en juridisk person behandlas. Det kan t.ex. vara fråga om organisationsnumret till en juridisk person som han eller hon äger eller företräder. Det kan också vara fråga om namnet på ett aktie- eller handelsbolag som den misstänkte driver verksamhet i eller någon annan liknande uppgift. Det kan även röra sig om juridiska personer i vilka den misstänkte använder bulvaner.

Punkten 8 tar sikte på uppgifter om särskilda grupperingar. Det kan exempelvis vara fråga om vissa ligor eller andra grupper som specialiserar sig på en särskild brottstyp och begår brott tillsammans i olika konstellationer. Ett annat exempel är grupper av brottsbelastade personer som tar sig särskilda namn för att markera gemenskap och som utnyttjar tillhörigheten till gruppen för att skrämma eller hota andra. Bland sådana grupperingar kan nämnas kriminella mc-gäng. Vid behandling av uppgifter av nu aktuellt slag måste bestämmelserna i 12 §, som reglerar behandling av känsliga personuppgifter, beaktas.

Enligt *punkten 9* får uppgifter om en misstänkts tillvägagångssätt också behandlas. Det kan t.ex. röra sig om en misstänkts sätt att maskera sig, att närma sig ett brottsoffer, att använda en viss typ av tillhygge eller vapen eller att använda visst brännbart material vid mordbränder. Uppgifter av det slaget kan användas bl.a. för att kontrollera om samma person kan ha gjort sig skyldig till andra brott än de som han eller hon misstänks för. Sådana uppgifter kan också användas för att knyta samman flera brott med okänd gärningsman.

Slutligen får enligt *punkten 10* registret innehålla uppgifter om nummer på det eller de ärenden där det finns uppgifter om den misstänkta personen. Det kan t.ex. vara fråga om diarienummer, referensnummer till underrättelseprojekt eller liknande.

10 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får behandlas i registret och om förfarandet vid registreringen.

Tillstånden till det nuvarande registret innehåller detaljerade bestämmelser i olika frågor, bl.a. om förfarandet vid registreringen. Vissa av dessa bestämmelser bör gälla även när registret lagregleras. Eftersom detalj-

regler av det slaget bör meddelas i förordning eller genom föreskrifter på lägre nivå informerar paragrafen om att närmare föreskrifter kan meddelas av regeringen, eller den myndighet som regeringen bestämmer. Frågan har behandlats i avsnitt 19.4.2.

Särskilda upplysningar

11 § Vid behandling av uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

I paragrafen, som har behandlats i avsnitt 19.6, uppställs ett krav på att personuppgifter som direkt kan hänföras till en person som inte själv är misstänkt för brott ska förses med en särskild upplysning om detta förhållande. Detta gäller dock bara i de fall där det inte finns någon misstanke alls. Upplysning behöver inte lämnas om det ändå framgår av omständigheterna att personen i fråga inte är misstänkt. Så är exempelvis fallet om personuppgiften rör ett brottsoffer. Bestämmelsen motsvarar i denna del 3 kap. 4 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I fråga om den närmare innebörden hänvisas till kommentaren till den paragrafen.

Behandling av känsliga personuppgifter

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

Om uppgifter om en person behandlas på annan grund, får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen.

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

Paragrafen anger i vilken utsträckning känsliga personuppgifter får behandlas. Frågan har behandlats i avsnitt 19.5. Bestämmelsen motsvarar i allt väsentligt 2 kap. 10 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För den närmare innebörden hänvisas till kommentaren till den bestämmelsen.

Tillgången till personuppgifter

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

I paragrafen föreskrivs att tillgången till personuppgifter i registret alltid ska begränsas till vad var och en behöver för att fullgöra sina arbetsuppgifter. Frågan har behandlats i avsnitt 19.7. En motsvarande bestämmelse finns i 2 kap. 11 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För den närmare innebörden hänvisas till kommentaren till den paragrafen.

Sökning

14 § Vid sökning i registret får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Det som anges i första stycket hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Paragrafen innehåller i *första stycket* ett förbud mot att använda känsliga personuppgifter som sökbegrepp i det allmänna spaningsregistret.

I *andra stycket* förtydligas att detta inte hindrar att brottsrubriceringar eller uppgifter som beskriver en persons utseende får användas som sökbegrepp. Begränsningar av samma slag finns i 3 kap. 5 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I fråga om den närmare innebörden hänvisas till kommentaren till den paragrafen. Frågan har behandlats i avsnitt 19.6.

15 § Uppgifter i registret som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara.

I paragrafen regleras vilka personuppgifter om icke misstänkta personer som får vara sökbara. Sådana uppgifter som direkt kan hänföras till en person, som inte misstänks för brott, får inte vara sökbara. Begränsningen omfattar således endast direkta personuppgifter. Däremot får uppgifter som indirekt rör en icke misstänkt person vara sökbara, t.ex. uppgifter om ett fordon som han eller hon är ägare till. Skälen till bestämmelsen har behandlats i avsnitt 19.6.

Utlämnande av personuppgifter och uppgiftsskyldighet

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

Paragrafen motsvarar 2 kap. 14 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Bestämmelsen är sekretessbrytande. Enligt paragrafen ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för att framställa statistiken. Enligt bilagan till förordningen (2001:100) om den officiella statistiken är Brottsförebyggande rådet statistikansvarig på rättsväsendets område utom vad gäller domstolarnas verksamhet.

17 § Om det är förenligt med svenska intressen, får personuppgifter lämnas till

1. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott, eller
2. en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organi-

sationer. Skälen för bestämmelsen har behandlats i avsnitt 19.7. Bestämmelsen motsvarar i sina huvuddrag 2 kap. 15 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Den som överväger att lämna ut en uppgift med stöd av paragrafen till en mottagare utanför EU och EES-området måste alltid enligt 33 och 34 §§ personuppgiftslagen (1998:204) försäkra sig om att den mottagande staten eller organisationen har en adekvat nivå på skyddet för personuppgifter.

Enligt *första stycket punkten 1* får personuppgifter lämnas ut till en utländsk polis- eller åklagarmyndighet om staten i fråga är ansluten till Interpol, eller till Interpol eller Europol. Uppgifter kan lämnas såväl efter förfrågan som utan föregående begäran. Förutsättningarna är dels att utlämnandet ska vara förenligt med svenska intressen, dels att uppgiften behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott.

Enligt *första stycket punkten 2* får personuppgifter lämnas till en utländsk myndighet eller mellanfolklig organisation om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Bestämmelsen är tillämplig om överenskommelsen ålägger Sverige att lämna vissa typer av uppgifter. Däremot gäller den inte för överenskommelser där det enbart sägs att utlämnande får ske.

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400), rätt att ta del av uppgifter i registret, om myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Regeringen meddelar föreskrifter om att uppgifter får lämnas ut i andra fall än som anges i första stycket.

Bestämmelser om att uppgifter får lämnas ut finns även i offentlighets- och sekretesslagen.

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande. Skälen för paragrafen har behandlats i avsnitt 19.7.

I *första stycket* regleras i vilken utsträckning uppgifter ur registret trots viss i paragrafen angiven sekretess får lämnas ut till andra brottsbekämpande myndigheter. Paragrafen har utformats som en uppgiftsskyldighet (jfr prop. 2007/08:160 s. 54). Den sekretessbrytande regeln omfattar dels sekretess enligt 21 kap. 3 § första stycket offentlighets- och sekretesslagen (2009:400), dels sekretess enligt 35 kap. 1 och 2 §§ samma lag. Sistnämnda paragrafer reglerar sekretess till skydd för enskild i bl.a. förundersökningar och andra brottsutredningar. Regeln har utformats efter mönster av bestämmelserna i 2 kap. 16–18 §§ i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Uppgifter ur registret får lämnas till övriga brottsbekämpande myndigheter, men endast om de har behov av uppgifterna i sin brottsbekämpande verksamhet. Behovet får i första hand bedömas med utgångspunkt i de uppgifter som den andra myndigheten har att sköta. Eftersom registret i huvudsak är personrelaterat, torde en begäran normalt avse en person som är föremål för misstanke, eller som av annat skäl är intressant i en utredning eller undersökning som bedrivs vid den andra myndigheten.

Det är den utlämnande myndigheten som avgör om den andra myndigheten behöver uppgiften för sin brottsbekämpande verksamhet. Uppgifter kan lämnas ut antingen på begäran av den andra myndigheten eller på polisens eget initiativ.

Med polismyndighet avses även Säkerhetspolisen när den för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet (se 7 § andra stycket polislagen [1984:387] jämförd med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen). När Säkerhetspolisen utför andra uppgifter (3 § samma förordning) är den en del av Rikspolisstyrelsen.

I *andra stycket* informeras om att regeringen har möjlighet att meddela föreskrifter om att uppgifter får lämnas ut i andra fall, t.ex. till någon av de uppräknade myndigheterna för något annat ändamål än som anges i första stycket.

Det *tredje stycket* innehåller en erinran om att det också finns bestämmelser om utlämnande av uppgifter i offentlighets- och sekretesslagen. En sådan bestämmelse är 8 kap. 3 §, som reglerar utlämnande till utländska myndigheter.

Elektroniskt utlämnande av personuppgifter

19 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Regeringen meddelar föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall.

Paragrafen reglerar under vilka förutsättningar personuppgifter får lämnas ut i elektronisk form på medium för automatiserad behandling, t.ex. på CD-rom, USB-minne eller i ett e-postmeddelande. Den motsvarar 2 kap. 20 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Innebörden är att en större mängd personuppgifter inte får lämnas ut på medium för automatiserad behandling, såvida inte regeringen har meddelat föreskrifter om detta. Däremot kan enstaka uppgifter lämnas ut. I fråga om vad som avses med enstaka uppgifter hänvisas till kommentaren till 2 kap. 20 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Av andra meningen framgår att regeringen har möjlighet att meddela föreskrifter om utlämnande på sådant medium även i andra fall. Frågan har behandlats i avsnitt 19.7.

20 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till registret.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Paragrafen innehåller bestämmelser om direktåtkomst. Frågan har behandlats i avsnitt 19.7.

Första stycket innebär att Rikspolisstyrelsen har möjlighet att besluta att vissa myndigheter får ha direktåtkomst till registret. De uppräknade

myndigheterna har alltså ingen absolut rätt att få sådan tillgång till registret. Bestämmelsen har sin motsvarighet i 3 kap. 8 § samt 4 kap. 10 och 17 §§ lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För en närmare beskrivning av innebörden av bestämmelsen hänvisas till kommentaren till 3 kap. 8 § den lagen. Som utvecklas i kommentaren till 18 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst.

I *andra stycket* slås fast att myndigheter som har medgetts direktåtkomst till registret ansvarar för att åtkomsten till uppgifterna i registret begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Regeln är tillämplig både på myndigheter inom polisväsendet och på andra myndigheter som kan medges direktåtkomst.

I *tredje stycket* informeras om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela närmare föreskrifter om direktåtkomsten samt om behörighet och säkerhet.

Gallring

21 § Uppgifter om en person som har registrerats enligt 5 § ska gallras senast tre år efter det att uppgiften om misstanke om brott registrerades. Om uppgiften avser misstanke om brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver uppgifterna inte gallras förrän fem år efter registreringen.

Om en ytterligare uppgift om personen förs in i registret, förlängs gallringsfristen med

1. fem år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. tre år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om annat brott än som anges i 1, eller
3. ett år från det att den nya uppgiften fördes in i registret, om uppgiften inte avser misstanke om brott.

Den tid då en person som har registrerats enligt 5 § avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i första och andra styckena.

Paragrafen, vars bakgrund har kommenterats i avsnitt 19.8, innehåller bestämmelser om gallring av uppgifter som har registrerats med stöd av 5 §. Bestämmelserna anger när en uppgift senast ska gallras, vilket innebär att uppgifterna kan gallras tidigare. Den frågan kan aktualiseras bl.a. om personen avlider eller om det av något annat skäl inte längre finns grund för att behandla uppgifter om personen i det allmänna spaningsregistret. Gallring kan också aktualiseras om det enligt 25 § har utfärdats föreskrifter om kortare gallringstid än vad som anges i paragrafen.

I *första stycket* föreskrivs att uppgifter om en person som avses i 5 §, dvs. en person som är misstänkt för brott, enligt huvudregeln ska gallras efter tre år. Är det fråga om ett brott med lägst två års fängelse i straffskalan får uppgifterna bevaras i fem år.

I *andra stycket* behandlas den situationen att nya uppgifter om en registrerad person tillförs registret. I sådana fall kan gallringsfristen komma att förskjutas framåt. Om uppgifterna består i nya brottsmisstankar för-

längs gallringsfristen med tre respektive fem år, beroende på brottets svårhetsgrad, räknat från den nya registreringen. Om den nya uppgiften inte avser en ny brottsmisstanke, utan exempelvis uppgifter om den misstänktes kontakter med andra misstänkta personer, förlängs gallringsfristen med ett år. Det innebär att om registret, beträffande en person som misstänks för ett brott som medför att uppgifterna ska gallras efter tre år, tillförs uppgift om ett nytt brott av samma svårhetsgrad ett år efter den ursprungliga registreringen så kommer uppgifterna om honom eller henne att kunna bevaras i sammanlagt fyra år, under förutsättning att inga nya brottsmisstankar eller andra noteringar tillkommer som kan förlänga tiden ytterligare. En registrering av en ny uppgift kan endast förlänga den ursprungliga gallringsfristen, inte förkorta den. Om t.ex. en notering enligt andra stycket 3 görs i början av en tre- eller femårsfrist kommer den således inte att påverka den totala bevarandetiden. Den nya uppgiften får dock bevaras lika länge som övriga uppgifter.

Det *tredje stycket* innehåller en bestämmelse som innebär att tidpunkten för gallring skjuts fram i de fall där den registrerade avtjänar fängelsestraff, genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning. En motsvarande bestämmelse finns i 3 kap. 14 § sjätte stycket lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

22 § Uppgifter om en person som avses i 6 § ska gallras senast när uppgifterna om den person som har registrerats enligt 5 § och som uppgifterna har samband med gallras.

I paragrafen regleras när uppgifter om personer som behandlas i registret med stöd av 6 §, dvs. personer som inte själva är misstänkta för brott, ska gallras. Sådana uppgifter ska gallras senast när uppgifterna om den misstänkte, som registreringen har samband med, gallras. Frågan har behandlats i avsnitt 19.8.

23 § Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats enligt 7 § ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver uppgifterna inte gallras förrän fem år efter det att den senaste uppgiften infördes.

Bakgrunden till paragrafen har tecknats i avsnitt 19.8. Den reglerar när uppgifter som har registrerats med stöd av 7 § ska gallras. Det rör sig om uppgifter om juridiska personer, transportmedel och andra föremål som kan antas ha samband med brott men där det inte finns någon person som är misstänkt för brottet. Sådana uppgifter gallras enligt huvudregeln tre år efter den senaste registreringen. Är det fråga om allvarligare brott, dvs. brott med lägst två års fängelse i straffskalan, får uppgifterna bevaras i fem år. Gallringstiden kan förlängas om registret, innan tiden har löpt ut, tillförs en ny uppgift angående det registrerade objektet.

24 § Om det finns synnerliga skäl, får regeringen, eller den myndighet som regeringen bestämmer, i ett enskilt fall besluta att en uppgift får bevaras under längre tid än vad som anges i 21–23 §§. Ett sådant beslut ska omprövas varje år.

Bakgrunden till paragrafen har behandlats i avsnitt 19.8.

I paragrafen öppnas en möjlighet att i ett enskilt fall besluta att uppgifter, som annars skulle ha gallrats, får bevaras. För ett sådant beslut krävs synnerliga skäl, vilket innebär att skälen ska vara mycket starka. Som exempel kan nämnas att det ibland kan finnas skäl att bevara uppgifter som rör vissa brottslingar under längre tid än vad som annars är tillåtet, om risken för återfall i brott bedöms vara särskilt stor. Det kan t.ex. gälla en sexualförbrytare som periodvis vårdas för psykisk sjukdom, och som av det skälet inte vistas ute i samhället och har möjlighet att begå nya brott, men där risken för att vederbörande senare begår nya brott är markant.

25 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om gallring.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att personuppgifter, med avvikelse från vad som anges i 21–23 §§, får bevaras för historiska, statistiska eller vetenskapliga ändamål.

I paragrafens *första stycke* informeras om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela närmare föreskrifter om gallring. Sådana föreskrifter kan avse att vissa uppgifter i registret ska gallras vid en tidigare tidpunkt.

Av paragrafens *andra stycke* följer att regeringen, eller den myndighet som regeringen bestämmer, också har möjlighet att meddela föreskrifter om att uppgifter ska bevaras för historiska, statistiska eller vetenskapliga ändamål, trots bestämmelserna i 21–23 §§ om gallring.

Rättelse och skadestånd

26 § Bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen.

Paragrafen, vars bakgrund har tecknats i avsnitt 19.9.1, reglerar en registrerad persons rätt till rättelse och skadestånd, om dennes personuppgifter har behandlats på ett felaktigt sätt. Genom hänvisningen till personuppgiftslagen (1998:204) regleras möjligheterna att agera vid felaktig personuppgiftsbehandling på samma sätt som i bl.a. lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister.

22.3 Förslaget till lag om ändring i rättegångsbalken

28 kap.

12 a § Kroppsbesiktning genom tagande av salivprov får göras på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera DNA-profilen i det DNA-register eller det utredningsregister som förs enligt lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Bakgrunden till ändringen, som har kommenterats i avsnitt 9.6 och 20, är att bestämmelserna om registrering i register över DNA-profiler har ändrats så att begreppet DNA-profil har ersatt uttrycket ”resultatet av DNA-analys”. En följdändring har gjorts i denna paragraf. Vidare har hänvisningen till polisdatalagen (1998:622) ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Även en språklig ändring har gjorts. Någon ändring i sak är inte avsedd.

12 b § Kroppsbesiktning genom tagande av salivprov får göras på annan än den som skäligen kan misstänkas för ett brott, om

1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och
2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.

Analysresultatet får inte jämföras med de DNA-profiler som finns registrerade i register över DNA-profiler som förs enligt lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller i övrigt användas för annat ändamål än det för vilket provet har tagits.

Första stycket gäller inte den som är under 15 år.

Paragrafen anger i vilka fall salivprov får tas på den som inte är skäligen misstänkt. I *första stycket* har en språklig ändring gjorts. *Tredje stycket* är oförändrat.

Av de skäl som anges i kommentaren till 12 a § har i *andra stycket* uttrycket ”resultatet av DNA-analys” ersatts med begreppet DNA-profil och registren benämns numera register över DNA-profiler. Hänvisningen till polisdatalagen (1998:622) har ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Någon ändring i sak är inte avsedd.

22.4 Förslaget till lag om ändring i vapenlagen (1996:67)

2 kap.

Utlämnande av personuppgifter och uppgiftsskyldighet

22 § Bestämmelserna om utlämnande av personuppgifter och uppgiftsskyldighet i 2 kap. 14 och 15 §§ lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet gäller även när personuppgifter behandlas i vapenregister enligt denna lag.

Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut även i andra fall.

Paragrafen, som är ny, har behandlats i avsnitt 6.3.

I *första stycket* anges att vissa av bestämmelserna om utlämnande av personuppgifter och uppgiftsskyldighet i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet även ska gälla vid behandling i vapenregistren. Paragraferna i fråga behandlar dels uppgiftsskyldighet till statistikmyndighet, dels utlämnande av uppgifter till utländsk myndighet och mellanfolklig organisation. För en närmare be-

skrivning av innebörden av bestämmelserna hänvisas till kommentaren till dessa paragrafer.

I *andra stycket* informeras om att regeringen har möjlighet att meddela föreskrifter om utlämnande även i andra fall.

22.5 Förslaget till lag om ändring i säkerhetsskyddslagen (1996:627)

12 § Med registerkontroll avses att uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och lagen (2010:000) om polisens allmänna spaningsregister. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

I paragrafen, som har kommenterats i avsnitt 20, anges vad som avses med registerkontroll. Liksom nu inrymmer registerkontroll att uppgifter hämtas från belastningsregistret och misstankeregistret. Vidare får uppgifter hämtas som behandlas enligt lagen om polisens allmänna spaningsregister. Hänvisningen till polisdatalagen (1998:622) har ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Ändringarna innebär att möjligheten att hämta uppgifter utökas i viss mån. Avsikten är emellertid inte att ändringarna ska innebära några praktiska förändringar av registerkontrollen.

21 § Utlämnande av uppgifter vid registerkontroll får omfatta

1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret och misstankeregistret samt uppgifter som behandlas hos Säkerhetspolisen.

Den tidigare hänvisningen till SÄPO-registret i punkten 2 har tagits bort, eftersom den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet inte innehåller några bestämmelser om ett sådant register. Någon ändring i sak är inte avsedd.

22 § Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret och misstankeregistret samt uppgifter som behandlas hos Säkerhetspolisen.

Ändringen är av samma slag som ändringen i 21 §.

22.6 Förslaget till lag om ändring i lagen (2000:344) om Schengens informationssystem

5 § Registret ska endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204),

lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller annan svensk författning.

I *första stycket* har endast en språklig ändring gjorts.

Ändringen i *andra stycket* består i att hänvisningen till polisdatalagen (1998:622) har ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

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

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 polisens behandling av personuppgifter enligt lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lagen (2010:000) om polisens allmänna spaningsregister. Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och 12 § lagen om polisens allmänna spaningsregister.

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Paragrafen reglerar Säkerhets- och integritetsskyddsnämndens tillsynsuppgifter. Ändringarna i *första* och *tredje styckena* är enbart språkliga.

Enligt *andra stycket* ingår det i nämndens uppgifter att utöva tillsyn över såväl Säkerhetspolisens som den övriga polisens personuppgiftsbehandling i den brottsbekämpande verksamheten. Tillsynen ska särskilt avse behandlingen av känsliga personuppgifter. Som utvecklas i avsnitt 17.2 ska tillsynen syfta till att säkerställa att personuppgiftsbehandlingen är författningsenlig. Hänvisningen till polisdatalagen (1998:622) har ersatts med hänvisningar till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lagen om polisens allmänna spaningsregister.

22.8 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

18 § Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i polisdatalagen (1998:622) och lagen (2000:344) om Schengens informationssystem.

Paragrafen reglerar sekretessgenombrott för uppgifter i angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Hänvisningen till 17 § har, av de skäl som angetts i avsnitt 20, ändrats till att omfatta endast andra stycket i den paragrafen.

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 denne 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, en polismyndighet, Skatteverket, Statens kriminaltekniska laboratorium, Tullverket eller Kustbevakningen,
5. Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller en polismyndighet i brottmål,
6. register som förs av Rikspolisstyrelsen enligt polisdatalagen (1998:622) eller som annars behandlas där med stöd av samma lag,
7. register som förs enligt lagen (1998:621) om misstankeregister,
8. register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,
9. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,
10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag, eller
11. register som förs enligt lagen (2010:000) 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 denne 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 denne 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.

Paragrafen reglerar sekretess för enskild i bl.a. förundersökningar och annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av polisen. Hänvisningen i *första stycket punkten 9* till 4 kap. samma lag har, av de skäl som angetts i avsnitt 20, ändrats till en hänvisning till 5 kap.

22.9 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

2 § Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 7 § 1 eller 5 kap. 1 § 1 lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet, 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

1. sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, eller
2. sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

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.

Paragrafen, som har behandlats i avsnitt 20, reglerar sekretess i underrättelseverksamhet. Eftersom sådan verksamhet inte regleras på samma sätt i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet som i polisdatalagen (1998:622) har omfattningen av sekretessen enligt *första stycket* formulerats om. Tillämpningsområdet är i huvudsak detsamma som tidigare.

Andra–fjärde styckena är oförändrade.

18 § Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Paragrafen reglerar sekretessgenombrott för uppgifter i angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Hänvisningen till polisdatalagen (1998:622) har ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

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 denne 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, en polismyndighet, Skatteverket, Statens kriminaltekniska laboratorium, Tullverket eller Kustbevakningen,
5. Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller en polismyndighet i brottmål,
6. register som förs av Rikspolisstyrelsen enligt lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag,
7. register som förs enligt lagen (1998:621) om misstankeregister,
8. register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

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

10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag, eller

11. register som förs enligt lagen (2010:000) 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 denne 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 denne 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.

Paragrafen reglerar sekretess i bl.a. förundersökningar och liknande utredningar.

I *första stycket punkten 6* har hänvisningen till polisdatalagen (1998:622) ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Enligt *punkten 11*, som är ny, gäller sekretess för uppgifter i register som förs enligt lagen om polisens allmänna spaningsregister. Registret regleras i likhet med misstankeregistret i en särskild punkt i paragrafen.

10 § 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,

3. enligt vad som föreskrivs i

– lagen (1998:621) om misstankeregister,

– lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,

– lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar,

– lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet,

– förordningar som har stöd i dessa lagar, eller

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

Paragrafen reglerar vissa undantag från sekretessen i 35 kap. 1 §. Den tidigare hänvisningen till polisdatalagen (1998:622) har ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

37 kap.

7 § Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och lagen (2010:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Paragrafen reglerar undantag från sekretess enligt 6 §. Ändringen är av samma slag som ändringen i 35 kap. 10 §.

Polisdatautredningens sammanfattning

Några utgångspunkter

Utredningens direktiv innebär ett uppdrag att följa genomförandet av den nya polisregisterlagstiftningen och att påtala eventuella brister särskilt från integritetssynpunkt. Utredningen skall överväga om det behöver vidtas några åtgärder, t.ex. i form av författningsändringar eller genom ökade möjligheter till insyn eller kontroll, för att lagstiftningen skall uppnå sitt syfte att öka möjligheten till effektiv brottsbekämpning och samtidigt värna om den enskildes personliga integritet.

Sedan den 1 april 1999 gäller en ny lag om behandling av personuppgifter hos polisen, polisdatalagen (1988:622). Den nya lagen bygger på personuppgiftslagen (1998:204) och innehåller bara de särregler som ansetts nödvändiga i polisens verksamhet. Polisdatalagen utgör en del av den nya lagstiftningen om behandling av personuppgifter i polisens verksamhet. Övriga lagar inom detta område utgörs av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och lagen (2000:344) om Schengens informationssystem.

Nämnda lagar har utgjort utgångspunkten för vårt arbete. Bland övriga rättskällor av betydelse bör särskilt nämnas Europolkonventionen, Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna samt Europarådets rekommendation om användningen av personuppgifter inom polissektorn m.m.

Målsättningen med våra förslag är att de skall utgöra en lämplig avvägning mellan polisens rätt att använda modern teknik och den enskildes integritet. En utgångspunkt för oss i arbetet har varit att hinder för ett rationellt utnyttjande av datorstöd inte bör ställas upp i större utsträckning än vad som är nödvändigt med hänsyn till intresset av skydd för den personliga integriteten.

Vi har i enlighet med direktiven inventerat de register som förs inom polisen. Den befintliga registerstrukturen har uppkommit främst som följd av Datainspektionens tillstånd för polisen att föra olika enskilda register och är således inte resultatet av någon övergripande planering.

Ett stort antal register förs, såväl centralt som lokalt. Registren kan indelas i tre grupper beroende på vilka bestämmelser som styr behandlingen, nämligen

– register som förs med stöd av särskilda regler i lagstiftningen,

– register som förs med stöd av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen, och

– register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av tillstånd från Datainspektionen.

Det traditionella registerbegreppet har vid flera tillfällen kritiserats. Dagens system inom polisen byggs företrädesvis som ärendehanteringssystem och inte som traditionella register. I ärendehanteringssystem lagras hela aktmaterial. Systemen är anpassade för fritextsökning. Vi finner dock inte anledning att i lagstiftningen ersätta begreppet register som beteckning för vissa fastställda informationsmängder med något annat begrepp.

Nya arbetsmetoder och ny teknik

Inom en mycket snar framtid lär praktiskt taget allt skrivarbete komma att utföras med hjälp av datorer. En realistisk lagstiftning måste ta hänsyn till de nya förhållandena. Manuell behandling av information, däribland personuppgifter, är inte längre ett realistiskt alternativ till automatiserad behandling av information. Den omständigheten att mängden automatiserat behandlade personuppgifter kraftigt ökat gör det ännu viktigare att en lagstiftning om behandling av personuppgifter i polisens verksamhet ger ett tillfredsställande skydd för den enskildes personliga integritet.

Polisen skall enligt nyare uttalanden från statsmakterna arbeta problemorienterat och verka brottsförebyggande. Arbetet skall vara proaktivt och inte reaktivt inriktat. För att kunna verka brottsförebyggande måste dock polisen inhämta och bearbeta information om enskilda personer i större utsträckning än som skedde vid ett traditionellt reaktivt arbetssätt. Det ligger därför i sakens natur att en brottsförebyggande arbetsmetod innebär ett ökat intrång i den enskildes personliga integritet i förhållande till ett reaktivt arbetssätt.

Användningen av digital teknik för behandling av ljud och bild är i hög grad ägnad att höja kvaliteten på polisens brottsutredningar. Detta gäller framför allt beträffande digitala bilder. Eftersom den digitala tekniken får anses utgöra automatiserad behandling blir dock bestämmelserna i personuppgiftslagen tillämpliga i den utsträckning behandlingen avser digitala bilder eller ljud som innehåller personuppgifter.

Polisens intranät används i första hand för att sprida verksamhetsrelaterad information inom polismyndigheterna.

Informationsutbytet med Europol

Sverige har anslutit sig till Europolkonventionen. Europols främsta uppgift är att vara ett kriminalunderrättelseorgan för de brottsbekämpande myndigheterna i medlemsländerna inom EU. Som sådant är Europol en knutpunkt för utbyte av information och underrättelser mellan medlemsländerna. Europol fungerar så att medlemsländerna tillhandahåller Europol uppgifter främst ur sina nationella polisregister. Dessa uppgifter bearbetas och analyseras sedan hos Europol. Resultatet av bearbetningen och analyserna delges därefter medlemsländerna.

Polisdatalagen medger inte att personuppgifter som härrör från kriminalunderrättelseverksamhet behandlas automatiserat annat än i särskilda undersökningar eller kriminalunderrättelseregister. Härigenom har informationsutbytet med Europol kommit att allvarligt försvåras.

En nordisk jämförelse

Som underlag för våra överväganden har vi inhämtat upplysningar om vilka regler som gäller i Danmark, Finland och Norge beträffande automatiserad behandling av personuppgifter i polisens verksamhet. Jämförelsen visar att den svenska lagstiftningen är mer restriktiv för polisen än de regleringar som gäller i de övriga nordiska länderna.

I enlighet med direktiven för utredningen har vi analyserat konsekvenserna av den nya regleringen om polisens rätt att behandla personuppgifter automatiserat. Vi har vid vår analys av lagstiftningen kommit fram till att det behöver göras ändringar av regleringen i polisdatalagen. Ändringarna som vi anser erfordras är relativt omfattande. Vi anser därför att en ny lag om behandling av personuppgifter i polisens verksamhet som ersätter den nuvarande polisdatalagen bör införas. Även den nya lagen bör ges namnet polisdatalagen.

De särskilda lagarna om belastningsregister, om misstankeregister och om Schengens informationssystem bör vara kvar oförändrade.

Den nya polisdatalagen bör vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som skall vara tillämpliga i polisens verksamhet.

Den nya lagens syfte bör liksom personuppgiftslagen vara att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Den nya lagen bör gälla vid behandling av personuppgifter i sådan polisverksamhet som avses i 2 § 1–3 polislagen (1984:387), dvs. i den egentliga polisverksamheten.

Lagen bör gälla vid behandling av personuppgifter i form av bilder eller ljud, dock ej vid sådan behandling som består i insamling av personuppgifter genom upptagning av bilder eller ljud. Lagen bör inte gälla vid insamling av personuppgifter genom teleavlyssning, teleövervakning eller kameraövervakning.

Det digitala referensbiblioteket över barnpornografiska framställningar som förs av Rikskriminalpolisen behöver inte regleras särskilt i lagstiftningen.

Den nya polisdatalagen bör gälla enbart i polisens verksamhet. Lagen bör därför inte omfatta Ekobrottsmyndigheten.

Grundläggande bestämmelser om behandling av personuppgifter i den nya polisdatalagen

Personuppgiftslagens *definitioner* av begreppen behandling av personuppgifter, blockering av personuppgifter, mottagare, personuppgifter, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsombud, tillsynsmyndigheten och tredje man samt polisdatalagens definition av begreppet DNA-analys bör finnas med även i en ny lag för polisen.

Bestämmelsen i 9 § personuppgiftslagen om *grundläggande krav på behandling av personuppgifter* bör även i fortsättningen gälla i polisens verksamhet. Även särbestämmelsen om *gallring* i 13 § polisdatalagen bör vara kvar.

Rikspolisstyrelsen bör även i fortsättningen vara ensam personuppgiftsansvarig för de centrala registren i polisens verksamhet. En bestämmelse som ger Rikspolisstyrelsen möjlighet att besluta verkställighetsföreskrifter bör ingå i en ny polisdataförordning.

Personuppgifter bör få behandlas endast *om behandlingen är nödvändig* för att polisen skall kunna utföra polisverksamhet som består i att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,

2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat eller

3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Den nya lagen bör inte hindra att personuppgifter *diarieförs* eller *behandlas i löpande text* om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

Bestämmelsen i 5 § polisdatalagen om behandling av *känsliga personuppgifter* bör gälla även i fortsättningen.

Bestämmelsen i 22 § personuppgiftslagen om behandling av *personnummer och samordningsnummer* bör gälla på polisområdet. Dock bör samtycke inte kunna åberopas som grund för behandling.

I 10 och 11 §§ polisdatalagen finns bestämmelser om *behandling av uppgifter om kvarstående misstankar*. Dessa bestämmelser bör oförändrat gälla även i fortsättningen.

Någon bestämmelse om förbud mot överföring av personuppgifter till tredjeland motsvarande 33 § personuppgiftslagen bör inte gälla i den egentliga polisverksamheten. En följd av detta blir att offentliga personuppgifter kan spridas på *Internet*. Av integritetsskäl bör dock en efterlysning av en person med anledning av att han eller hon avvikit från verkställande av påföljd för brott eller med anledning av att han eller hon misstänks för brott, få ske på Internet endast om

1. domen eller misstanken avser ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet, eller

2. personen kan antas vara farlig för annans personliga säkerhet.

Reglerna i 23–27 §§ personuppgiftslagen om *information till registrerade* bör även i fortsättningen gälla i polisens verksamhet. Det behövs dock därutöver ytterligare två undantag från polisens informationsplikt. I fall uppgifter om en enskild person samlas in från personen själv, bör information heller inte behöva lämnas, om

– det finns bestämmelser om antecknandet eller utlämnandet av personuppgifter i författning, eller

– uppgifterna samlas in i samband med larm eller annan liknande underrättelse och larmet eller underrättelsen kräver omedelbara insatser från den personuppgiftsansvarige.

I stället för att som i dag avse registrerade bör bestämmelserna i den nya lagen om information avse enskilda.

Bestämmelserna i 28 § personuppgiftslagen om *rättelse* bör även i fortsättningen gälla på polisområdet. Bestämmelserna bör dock avse den enskilde i stället för den registrerade.

När det gäller *säkerheten vid behandling* bör liksom i dag bestämmelserna i 30–32 §§ personuppgiftslagen gälla i polisens verksamhet. Regeln i 32 § om tillsynsmyndighetens rätt att besluta om säkerhetsåtgärder bör dock meddelas genom förordning. Därutöver bör det i den nya lagen finnas en bestämmelse som föreskriver att *direkt åtkomst* till personuppgifter skall vara förbehållen de personer inom polisen som på grund av sina arbetsuppgifter behöver tillgång till information om uppgifterna.

Bestämmelsen i 8 § personuppgiftslagen om *förhållandet till offentlighetsprincipen* bör liksom i dag gälla för polisen.

I 6–8 §§ polisdatalagen och i 15–16 §§ polisdataförordningen finns bestämmelser om *utlämnande av uppgifter*. Bestämmelserna bör oförändrade föras över till en ny polisdatalag respektive en ny polisdataförordning.

Bestämmelserna i 36–41 §§ personuppgiftslagen och 3–7 §§ personuppgiftsförordningen om *anmälan till tillsynsmyndigheten* och personuppgiftsombudets uppgifter, i 13 § personuppgiftsförordningen om bemyndiganden, i 2 § polisdataförordningen om förhandskontroll, och i 14 § polisdataförordningen om underrättelseskyldighet bör gälla även i fortsättningen för polisen.

Om den personuppgiftsansvarige har utsett ett personuppgiftsombud och anmälan därför inte behöver göras, bör *anmälan* i stället göras *till personuppgiftsombudet*. En ny polisdatalag bör innehålla en bestämmelse härom.

Bestämmelsen i 42 § personuppgiftslagen om upplysningar till allmänheten om behandlingar som inte anmälts bör gälla för polisen.

Personuppgiftslagens bestämmelser i 43–47 §§ personuppgiftslagen och i 2 § personuppgiftsförordningen om *Datainspektionens befogenheter* bör gälla på polisområdet. Bestämmelserna bör dock meddelas i förordning.

Bestämmelserna i 48 § personuppgiftslagen och i 9 § polisdatalagen om *skadestånd* bör gälla för polisen också i fortsättningen. Den nya regeln bör dock avse enskilda och inte registrerade. Någon *straffbestämmelse* motsvarande 49 § personuppgiftslagen behövs inte i den nya lagen.

Bestämmelserna i 51 § personuppgiftslagen om *överklagande* bör i sak gälla även i fortsättningen för polisen. Dessutom bör det i en ny lag föreskrivas att en myndighets beslut om rättelse och om information som skall lämnas efter ansökan skall överklagas hos kammarrätten.

Behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot

Vid utformningen av en lag om behandling av personuppgifter i polisens verksamhet måste beaktas att polisens arbete skall vara inriktat främst på brottsförebyggande verksamhet.

Polisdatalagen innehåller en reglering om behandling av personuppgifter i kriminalunderrättelseverksamhet och i kriminalunderrättelseregister. Regleringen har kommit att försvåra polisens arbete med att verka problemorienterat och brottsförebyggande.

En lag om behandling av personuppgifter bör handla om just behandling av personuppgifter och inte vara inriktad på att reglera vissa verksamheter eller arbetsmetoder hos polisen. Bestämmelserna om kriminalunderrättelseverksamhet och kriminalunderrättelseregister bör bl.a. av det skälet inte vara kvar i en ny polisdatalag. Bestämmelserna härom bör i stället ersättas av bestämmelser om behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot.

De personuppgifter som kommer att omfattas av sistnämnda regler är först och främst sådana som avser personer som inte är misstänkta för något konkret brott, men väl för att ha utövat eller utöva brottslig verksamhet. Uppgifterna kan dock även avse andra personer, t.ex. personer

som lämnat upplysningar om iakttagelser m.m. utan att själva vara misstänkta.

Uppgifter om en enskild person som det inte finns någon misstanke om brott mot bör få behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer.

Alla uppgifter som är nödvändiga för ändamålet med behandlingen bör få behandlas. Om uppgifter om en person som det över huvud taget inte finns någon misstanke mot behandlas, bör uppgiften förses med en anteckning om detta förhållande. Vid aktuell behandling av personuppgifter bör uppgifterna förses med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Aktuell behandling av personuppgifter bör få ske för att underlätta övervakning av personer som kan antas komma att begå brott. Behandling i detta syfte bör dock endast få avse dömda personer som antingen är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

Den personuppgiftsansvarige bör särskilt besluta de ändamål och villkor i övrigt som behövs för att förebygga otillbörligt intrång i enskildas personliga integritet. När det gäller villkor i övrigt kan det t.ex. röra sig om hur information skall inhämtas, hur arbetet skall ske och avrapporteras samt säkerheten vid behandling m.m.

Personuppgifter som behandlas enligt här aktuella bestämmelser bör få bevaras högst tre år från det att uppgifterna om personen samlades in. Uppgifter som behandlas för att underlätta övervakning av personer som kan antas komma att begå brott bör dock få bevaras till dess att uppgifterna gallras ur belastningsregistret.

Bestämmelserna om aktuell behandling av personuppgifter bör inte gälla personuppgifter

– i en förundersökning, eller

– i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Det allmänna spaningsregistret

Det föreligger ett mycket stort behov av det allmänna spaningsregistret (ASP) inom brottsbekämpningen. ASP är viktigt bl.a. för att närpolisverksamheten skall kunna fungera.

Det bör i den nya polisdatalagen införas särskilda regler om ASP. Lagregleringen bör i allt väsentligt ge polisen rätt att fortsätta den behandling av personuppgifter som i dag förekommer.

ASP bör få föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott. Bestämmelserna i den nya polisdatalagen om behandling av uppgifter om kvarstående misstankar bör inte gälla vid behandling av personuppgifter i ASP.

I ASP bör uppgifter som kan hänföras till en enskild person få föras in endast om den som avses med uppgiften kan misstänkas för att ha begått ett brott och om registreringen är av särskild betydelse för brottsbekämp-

ningen. Uppgifter om transportmedel eller andra varor som kan antas ha samband med brott bör få registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna skall därvid förses med en upplysning om att det inte finns någon misstanke mot denne. I lagen bör vidare anges vilka typer av personuppgifter som får eller skall registreras i ASP.

Personuppgifter i ASP bör som regel gallras senast tre år efter det att uppgifter om att den registrerade kan misstänkas för att ha begått brott senast infördes. Om den senaste händelsen avser misstanke om ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet bör dock uppgifterna få stå kvar i fem år efter den senaste registreringen.

Uppgifter ur ASP bör under vissa förutsättningar få lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet. Polismyndigheterna bör få ha direkt åtkomst till uppgifter i ASP.

Ytterligare bestämmelser om vissa register m.m.

Den nya polisdatalagen bör utöver regler om ASP innehålla särskilda regler om register med uppgifter om DNA-analyser i brottmål och om fingeravtrycks- och signalementsregister.

Bestämmelserna i 22–28 §§ polisdatalagen och i 11 § polisdataförordningen om register med uppgifter om DNA-analyser i brottmål bör gälla även i fortsättningen.

Särskilda författningsregler om den behandling av personuppgifter i Statens kriminaltekniska laboratoriums verksamhet som sker med anledning av laboratoriets DNA-analyser bör inte införas.

Bestämmelserna i 29–31 §§ polisdatalagen om fingeravtrycks- och signalementsregister bör gälla även i fortsättningen. Sådana register bör dock utöver vad som framgår av 30 § polisdatalagen även få innehålla uppgifter om brottskoder.

Det behövs inte någon särskild författningsreglering för eventuella centrala system motsvarande de lokala system som i dag används, t.ex. rationell anmälningsrutin (RAR), datoriserad utredningsrutin – tvångsmedel (DurTvå) och kommunikationscentralernas system (KC-systemen).

Säkerhetspolisen

En ändring av Säkerhetspolisens organisation bestående i en sammanslagning mellan Säkerhetspolisen och Rikskriminalpolisen övervägs för närvarande. Våra förslag utgår från den nuvarande organisationen av Säkerhetspolisen.

Bestämmelserna i den nya polisdatalagen om behandling av personuppgifter i Säkerhetspolisens verksamhet bör i huvudsak ha samma innebörd som i dag. Den särskilda lagregleringen om SÄPO-registret bör dock inte vara kvar i den nya lagen. Några särskilda registerbestämmelser för Säkerhetspolisen bör inte heller i övrigt införas.

Säkerhetspolisen bör få behandla personuppgifter för att underlätta

– spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,

– spaning i syfte att bekämpa terrorism och
– registerkontroll enligt säkerhetsskyddslagen.

Bestämmelserna i den nya polisdatalagen om behandling av uppgifter om kvarstående misstankar och om behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot bör inte gälla för Säkerhetspolisen.

Ikraftträdande

Den nya polisdatalagen bör kunna träda i kraft den 1 juli 2003, då polisdatalagen (1998:622) bör upphöra att gälla. Vi har bedömt att några övergångsbestämmelser till den nya lagen inte behövs.

Konsekvenser

Vi har genomfört konsekvensanalyser enligt 14 och 15 §§ kommittéförordningen (1998:1474). Våra förslag bör ge polisen bättre förutsättningar att arbeta problemorienterat och verka brottsförebyggande.

Enligt vår bedömning ger de förslag som vi lämnar inte upphov till kostnader som inte ryms inom berörda myndigheters anslag. Förslagen i övrigt får inte några sådana konsekvenser som motiverar en särskild redovisning.

Polisdatautredningens lagförslag

1 Förslag till polisdatalag

Härigenom föreskrivs följande.

1 kap. Lagens syfte och tillämpningsområde

Syftet med lagen

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i polisens verksamhet.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i polisens verksamhet för att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat eller
3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Lagen gäller också behandling av sådana uppgifter som avses i 5 kap. 10 och 11 §§.

3 § Lagen gäller inte för behandling av personuppgifter som företas med stöd av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2000:344) om Schengens informationssystem.

Lagen gäller heller inte vid insamling av personuppgifter genom teleavlyssning, teleövervakning eller kameraövervakning. Lagen gäller vid övrig behandling av personuppgifter i form av bilder eller ljud, dock ej vid sådan behandling som består i insamling av personuppgifter genom upptagning av bilder eller ljud.

Vid behandling av personuppgifter i form av bilder eller ljud skall vad som i lagen sägs om insamling tillämpas när uppgifterna första gången behandlas efter det att insamlingen avslutats.

4 § Vid annan behandling av personuppgifter i polisens verksamhet än som avses i 2 eller 3 § gäller personuppgiftslagen (1998:204).

5 § Bestämmelserna i 1 och 2 kap., 3 kap. 1 och 2 §§, 4 kap. samt 6 och 7 kap. gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad samt även för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 3 kap. 3–11 §§ och 5 kap. gäller endast automatiserad behandling av personuppgifter.

Definitioner

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

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

svariges räkning.

Personuppgiftsombud

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

2 kap. Grundläggande principer vid behandling av personuppgifter

Grundläggande krav på behandlingen av personuppgifter

1 § Den personuppgiftsansvarige skall se till att

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

Vad som sagts i första stycket 9 gäller inte personuppgifter

1. i en förundersökning, eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

2 § Vid tillämpning av 1 § första stycket 4 gäller att en behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte skall anses som oförenlig med de ändamål för vilka uppgifterna samlades in.

Personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid än som sagts i 1 § första stycket 9. Personuppgifterna får dock i sådana fall inte bevaras under en längre tid än vad som behövs för dessa ändamål.

Personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål får användas för att vidta åtgärder i fråga om den enskilde bara om den enskilde har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den enskildes vitala intressen.

3 § Personuppgifter får behandlas bara om behandlingen är nödvändig för att sådan polisverksamhet som anges i 1 kap. 2 § första stycket skall kunna utföras.

Lagen hindrar inte att personuppgifter diarieförs eller behandlas i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

3 kap. Vissa behandlingar av personuppgifter

Behandling av känsliga personuppgifter

1 § 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 sexuella läggning.

Om uppgifter om en person behandlas på annan grund får uppgifterna kompletteras med sådana uppgifter som avses i första stycket, om det är oundgängligen nödvändigt för syftet med behandlingen.

Behandling av personnummer

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

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

Behandling av uppgifter om kvarstående misstankar

3 § Om en förundersökning mot en person har lagts ned på grund av bristande bevisning får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast under förutsättning att

1. den misstänkte enligt förundersökningsledarens bedömning fortfarande är skäligen misstänkt för brottet och
2. uppgifterna behövs för att förundersökningen skall kunna tas upp på nytt.

4 § Om åtal mot en person har lagts ned eller om denne genom lagakraftvunnen dom har frikänts får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast

1. om förundersökningen tas upp på nytt eller
2. för prövning av ett särskilt rättsmedel enligt 58 kap. rättegångsbalken.

Behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot

Syften med behandlingen

5 § Uppgifter om en enskild person som det inte finns någon misstanke om brott mot får behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer.

Uppgifter om en enskild person som det inte finns någon misstanke mot skall förses med en upplysning om detta förhållande.

6 § Personuppgifter som behandlas enligt 5 § skall förses med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

7 § Personuppgifter som behandlas enligt 5 § för att underlätta övervakning av personer som kan antas komma att begå brott får endast avse dömda personer som är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

Beslut om villkor för behandlingen

8 § Den personuppgiftsansvarige skall särskilt besluta ändamål för behandlingen av personuppgifter och de villkor i övrigt som behövs för att förebygga otillbörligt intrång i enskildas personliga integritet.

Gallring

9 § Personuppgifter som behandlas enligt 5 § får inte bevaras längre tid än tre år från det att uppgifterna om personen samlades in. Sådana personuppgifter som avses i 7 § får dock bevaras senast till dess att uppgifterna om personen gallras ur belastningsregistret.

Regeringen, eller den myndighet regeringen bestämmer, får meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Behandling av personuppgifter som inte omfattas av bestämmelserna

10 § Bestämmelserna i 5–9 §§ gäller inte behandling av personuppgifter

1. i en förundersökning eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Behandling av uppgifter på Internet om efterlysningar av enskilda personer

11 § En efterlysning av en person med anledning av att han eller hon avvikit från verkställighet av påföljd för brott eller med anledning av att

han eller hon misstänks för brott, får göras allmänt tillgänglig på Internet endast om

1. domen eller misstanken avser ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet eller
2. personen kan antas vara farlig för annans personliga säkerhet.

4 kap. Särskilt om behandling av personuppgifter hos Säkerhetspolisen

1 § Säkerhetspolisen får utan hinder av bestämmelserna i 3 kap. 3–10 §§ behandla personuppgifter för att underlätta

1. spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
2. spaning i syfte att bekämpa terrorism och
3. registerkontroll enligt säkerhetsskyddslagen (1996:627).

5 kap. Register

Spaningsregister

Ändamål

1 § Rikspolisstyrelsen får föra ett allmänt spaningsregister för polisens spaningsverksamhet. Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

2 § Det allmänna spaningsregistret får föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott.

Innehåll

3 § Det allmänna spaningsregistret får innehålla uppgifter som kan hänföras till en enskild person endast om den som avses med uppgiften kan misstänkas för att ha begått ett brott och om registreringen är av särskild betydelse för brottsbekämpningen.

Uppgifter om transportmedel eller andra varor som kan antas ha samband med ett brott eller om hjälpmedel som kan antas ha använts i samband med ett brott får registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna skall därvid förses med upplysning om att det inte finns någon misstanke mot denne.

4 § Det allmänna spaningsregistret får innehålla följande uppgifter om en enskild person:

1. upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet,
2. identifieringsuppgifter,
3. vistelseadress,
4. uppgifter om särskilda fysiska kännetecken,
5. uppgifter om verkställighet av påföljd för brott,

6. uppgifter om varor, brottshjälpmedel och transportmedel,
7. ärendenummer och
8. varning om att personen tidigare varit beväpnad, våldsam eller flyktbenägen.

Det allmänna spaningsregistret skall alltid innehålla uppgifter om de omständigheter och händelser som gett anledning att anta att den registrerade begått brott.

Gallring

5 § Uppgifter i det allmänna spaningsregistret om en registrerad person skall gallras senast tre år efter det att uppgifter om att denne kan misstänkas för att ha begått ett brott senast infördes. Om den senast införda uppgiften avser misstanke om ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet behöver dock uppgifterna inte gallras förrän fem år efter att den senaste uppgiften infördes.

Regeringen, eller den myndighet regeringen bestämmer, får meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål.

Bestämmelser som inte gäller

6 § Bestämmelserna i 3 kap. 3 och 4 §§ gäller inte vid behandling av personuppgifter i det allmänna spaningsregistret.

Register med uppgifter om DNA-analyser i brottmål

Ändamål

7 § Uppgifter om resultat av DNA-analyser får behandlas endast för att underlätta identifiering av personer i samband med utredning av brott. Rikspolisstyrelsen får föra register (DNA-register och spårregister) i enlighet med 8–12 §§ över de uppgifter som behandlas. Rikspolisstyrelsen är personuppgiftsansvarig för behandling av uppgifter i registren.

Sådana uppgifter som avses i första stycket får även behandlas i
1. i en förundersökning eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

DNA-register

8 § Ett DNA-register får innehålla uppgifter om resultatet av DNA-analyser som har gjorts under utredning av ett brott och som avser personer som har dömts för

1. ett sådant brott mot en persons liv eller hälsa, personliga integritet eller säkerhet som avses i 3, 4, 6, 8, 12 eller 17 kap. brottsbalken, om brottet kan leda till fängelse i mer än två år,
2. ett allmänfarligt brott som avses i 13 kap. brottsbalken, om brottet kan leda till fängelse i mer än två år, eller

3. försök, förberedelse, stämpling, anstiftan eller medhjälp till ett sådant brott som avses i 1 eller 2.

9 § Registreringen av ett analysresultat skall begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser.

Spårregister

10 § Ett spårregister får innehålla uppgifter om DNA-analyser som har gjorts under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver uppgifter om analysresultat får ett spårregister endast innehålla upplysningar som visar i vilket ärende analysen har gjorts.

11 § Uppgifter i spårregister får endast jämföras med analysresultat

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är misstänkt för brott.

Gallring

12 § Uppgifter i DNA-registret skall gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i spårregister skall gallras senast trettio år efter registreringen.

Prover från personer som inte är misstänkta för brott

13 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys från någon som inte är misstänkt för brottet får provet inte användas för något annat ändamål än det för vilket det togs. Ett sådant prov får inte heller sparas efter det att målet slutligt har avgjorts.

Fingeravtrycks- och signalementsregister

Ändamål

14 § För att underlätta identifiering av personer i samband med brott får Rikspolisstyrelsen behandla uppgifter i fingeravtrycks- och signalementsregister. Ett sådant register får användas för identifiering av okända personer även i andra fall. Rikspolisstyrelsen är personuppgiftsansvarig för behandling av uppgifter i registren.

Sådana uppgifter som avses i första stycket får även behandlas i

1. i en förundersökning eller

2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Uppgifter som får behandlas

15 § Fingeravtrycks- och signalementsregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I ett sådant register får endast antecknas uppgifter om

1. fingeravtryck,
2. signalement,
3. identifieringsuppgifter,
4. ärendenummer och
5. brottskoder.

Gallring

16 § Uppgifter i fingeravtrycks- eller signalementsregister om en misstänkt person skall gallras när förundersökning eller åtal mot personen läggs ned eller när åtal ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den registrerade skall behandlas med stöd av 3 kap. 3 och 4 §. När dessa uppgifter gallras skall även uppgifter i fingeravtrycks- och signalementsregister gallras.

Om den registrerade döms skall uppgifterna i registret gallras senast vid den tidpunkt då uppgifterna gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Regeringen får meddela föreskrifter om gallring av uppgifter om den som har lämnat fingeravtryck enligt lagen (1991:572) om särskild utlänningskontroll.

6 kap. Information till den enskilde, rättelse och säkerheten vid behandling

Information till den enskilde

Information som skall lämnas självmant

1 § Om uppgifter om en enskild person samlas in från personen själv, skall den personuppgiftsansvarige i samband därmed självmant lämna den enskilde information om behandlingen av uppgifterna.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om antecknandet eller utlämnandet av personuppgifterna i författning.

Information enligt första stycket behöver heller inte lämnas om uppgifterna samlas in i samband med ett larm eller en annan liknande underrättelse och larmet eller underrättelsen kräver omedelbara insatser från den personuppgiftsansvarige.

2 § Om personuppgifterna har samlats in från någon annan källa än den enskilde, skall den personuppgiftsansvarige självmant lämna den enskilde information om behandlingen av uppgifterna när de antecknas. Är uppgifterna avsedda att lämnas ut till tredje man, behöver informationen dock inte ges förrän uppgifterna lämnas ut för första gången.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om antecknandet eller utlämnandet av personuppgifterna i författning.

Information behöver inte heller lämnas enligt första stycket, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Om uppgifterna används för att vidta åtgärder som rör den enskilde, skall dock information lämnas senast i samband med att så sker.

Vad informationen skall omfatta

3 § Information enligt 1 eller 2 § skall omfatta

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

Information behöver dock inte lämnas om sådant som den enskilde redan känner till.

Information som skall lämnas efter ansökan

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

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

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

Information enligt första stycket behöver inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

5 § I den utsträckning det är särskilt föreskrivet i författning eller i beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den enskilde gäller inte bestämmelserna i 1–4 §§.

Rättelse

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

Säkerheten vid behandling

7 § 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.

Det skall finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 8 § första stycket.

Om det i annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i polisens verksamhet i frågor som avses i första stycket, skall dessa gälla i stället för vad som sägs i första stycket.

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

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

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

9 § Direkt åtkomst till personuppgifter skall vara förbehållen de personer inom polisen som på grund av sina arbetsuppgifter behöver tillgång till uppgifterna.

7 kap. Övriga bestämmelser

Förhållandet till offentlighetsprincipen

1 § Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka Rikspolisstyrelsens eller en polismyndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Bestämmelserna hindrar inte heller att Rikspolisstyrelsen eller en polismyndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Bestämmelserna i 2 kap. 2 § tredje stycket gäller inte för Rikspolisstyrelsens eller en polismyndighets användning av personuppgifter i allmänna handlingar.

Utlämnande av uppgifter

2 § Uppgifter som är nödvändiga för att framställa rättsstatistiken skall lämnas till den myndighet som ansvarar för att framställa sådan statistik.

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

Regeringen får meddela föreskrifter om att uppgifter på begäran får lämnas till polis- eller åklagarmyndighet i en stat som är ansluten till Interpol om det behövs för att myndigheten eller organisationen skall kunna förebygga, upptäcka, utreda eller beivra brott.

Uppgifter får vidare lämnas ut enligt vad som framgår av 1 kap. 3 § tredje stycket sekretesslagen (1980:100).

4 § Regeringen får meddela föreskrifter om att uppgifter får lämnas ut även i andra fall än som sägs i 2 och 3 §§.

Anmälan till tillsynsmyndigheten

Anmälningsskyldighet

5 § Behandling av personuppgifter som är helt eller delvis automatiserad omfattas av anmälningsskyldighet. Den personuppgiftsansvarige skall göra en skriftlig anmälan till tillsynsmyndigheten innan en sådan behandling eller en serie av sådana behandlingar med samma eller liknande ändamål genomförs.

Om den personuppgiftsansvarige utser ett personuppgiftsombud skall detta anmälas till tillsynsmyndigheten. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från anmälningsskyldigheten enligt första

stycket för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten.

Om det finns ett personuppgiftsombud skall anmälan göras till personuppgiftsombudet

6 § Om den personuppgiftsansvarige har anmält till tillsynsmyndigheten att ett personuppgiftsombud utsetts och vem det är, behöver anmälan enligt 5 § första stycket inte göras till tillsynsmyndigheten. Anmälan om sådan behandling av personuppgifter som avses i 5 § första stycket skall då i stället göras till personuppgiftsombudet.

Personuppgiftsombudets uppgifter

7 § Personuppgiftsombudet skall ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för honom eller henne.

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

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

8 § Personuppgiftsombudet skall föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som omfattas av anmälningsskyldighet till tillsynsmyndigheten eller till personuppgiftsombudet. Förteckningen skall omfatta åtminstone de uppgifter som en anmälan enligt 5 § skulle ha innehållit.

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

Förhandskontroll av särskilt integritetskänsliga behandlingar

10 § Regeringen får meddela föreskrifter om att sådana behandlingar av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten skall för förhandskontroll anmälas till tillsynsmyndigheten enligt 5 § tre veckor i förväg. Om regeringen har meddelat sådana föreskrifter, gäller inte undantaget från anmälningsskyldigheten till tillsynsmyndigheten enligt 6 §.

Upplysningar till allmänheten om behandlingar som inte anmälts

11 § Den personuppgiftsansvarige skall till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana automatiserade eller andra behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna skall omfatta det som en anmälan enligt 5 § första stycket skulle ha omfattat. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Skadestånd

12 § Den personuppgiftsansvarige skall ersätta den enskilde för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.

Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Detta gäller dock inte vid behandling av personuppgifter enligt konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.

Överklagande

13 § Tillsynsmyndighetens beslut enligt förordning som har meddelats för verkställighet av denna lag om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndigheten får bestämma att dess beslut skall gälla även om det överklagas.

14 § Rikspolisstyrelsens eller en polismyndighets beslut om rättelse och om information som skall lämnas enligt 6 kap. 4 § överklagas till kammarrätten.

Denna lag träder i kraft den 1 juli 2003, då polisdatalagen (1998:622) upphör att gälla.

2 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap 1 och 7 §§, 7 kap. 41 § och 9 kap. 17 § sekretesslagen (1980:100) skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 kap.

1 §

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,

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

3. verksamhet som rör utredning i frågor om näringsförbud,

4. åklagarmyndighets, polismyndighets, skattemyndighets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, eller

5. Finansinspektionens verksamhet som rör övervakning enligt insiderstrafflagen (2000:1086),

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till *sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till* Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Det samma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar samt sådan underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

För uppgift som hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Det samma gäller uppgift som hänför sig till sådan *underrättelseverksamhet som bedrivs av polisen,* sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar samt sådan underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, skatte-

myndighet, Tullverket eller Kustbevakningen med att uppdaga, utreda eller beivra brott samt hos tillsynsmyndighet i konkurs och inom exekutionsväsendet för uppgift som angår misstanke om att en gäldenär har begått brott som avses i 11 kap. brottsbalken eller annat brott som har samband med gäldenärens näringsverksamhet.

I fråga om uppgift i allmän handling som hänför sig till sådan underrättelseverksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

7 §

Sekretess gäller i verksamhet som avser rättslig hjälp på begäran av annan stat för uppgift som hänför sig till

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som angår tvångsmedel,

om det kan antas att den rättsliga hjälpen begärts under förutsättning att uppgiften inte röjs.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622)* och lagen om Schengens informationssystem.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (0000:00)* och lagen om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst fyrtio år.

7 kap.

41 §

Sekretess gäller hos polismyndighet och åklagarmyndighet, samt hos Rikspolisstyrelsen, Tullverket, Kustbevakningen och Migrationsverket, för uppgift om enskilds personliga förhållanden i en angelägenhet som avser en framställning enligt 3 § lagen (2000:344) om Schengens informationssystem

1. om omhändertagande av en person som har efterlysts för utlämning,
2. om att en person skall nekas tillträde till eller uppehållstillstånd i Schengenstaterna (spärrlista),
3. om tillfälligt omhändertagande av en person med hänsyn till dennes eller någon annans säkerhet, samt
4. om dold övervakning eller särskilda kontrollåtgärder, om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon honom närstående lider men.

Sekretess gäller hos myndighet som prövar ansökningar om visering och uppehållstillstånd för uppgift om enskilds personliga förhållanden i

en angelägenhet som avser en sådan framställning som avses i första stycket 2 under samma förutsättningar som anges i första stycket.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622)* och lagen (2000:344) om Schengens informationssystem.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (0000:00)* och lagen (2000:344) om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

9 kap.

17 §

Sekretess gäller för uppgift om enskilds personliga och ekonomiska förhållanden, om inte annat följer av 18 §

1. i utredning enligt bestämmelserna om förundersökning i brottmål,
2. i angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,
3. i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),
4. i åklagarmyndighets, polismyndighets, skattemyndighets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,
5. i Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller polismyndighet i brottmål,
6. i register som förs av Rikspolisstyrelsen enligt *polisdatalagen (1998:622*) eller som annars behandlas där med stöd av samma lag,

6. i register som förs av Rikspolisstyrelsen enligt *polisdatalagen (0000:00)* eller som annars behandlas där med stöd av samma lag,

7. i register som förs enligt lagen (1998:621) om misstankeregister,
8. i register som förs av Riksskatteverket enligt lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,
9. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,
10. i register som förs av Tullverket enligt lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag,

om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

Sekretess gäller i verksamhet, som avses i första stycket, för anmälan eller utsaga från enskild, om det kan antas att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs.

Utan hinder av sekretessen får en skadelidande, eller den som den skadelidande överlåtit sin rätt till, ta del av en uppgift

1. i en nedlagd förundersökning eller i en förundersökning som avslutats med ett beslut om att åtal inte skall väckas,
2. i en annan brottsutredning som utförts enligt bestämmelserna i 23 kap. rättegångsbalken och som avlutats på annat sätt än med beslut att

väcka åtal, med strafföreläggande eller med föreläggande av ordningsbot, eller

3. i en avslutad utredning enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, om den skadelidande, eller den som den skadelidande överlåtit sin rätt till, behöver uppgiften för att kunna få ett anspråk på skadestånd eller på bättre rätt till viss egendom tillgodosett och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående till honom att den inte lämnas ut.

Utan hinder av sekretessen får en uppgift också lämnas ut

1. till enskild enligt vad som föreskrivs i den särskilda lagstiftningen om unga lagöverträdare,

2. till enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) samt i förordning som har stöd i den lagen,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen (1998:622)*, lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar och i lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen (0000:00)*, lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar och i lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar,

4. till enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

Utan hinder av sekretessen får polisen på begäran av en enskild som lidit person- eller sakskada vid en trafikolycka lämna uppgift om identiteten hos en trafikant som haft del i olyckan.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

---

1. Denna lag träder i kraft den 1 juli 2003.

2. Äldre bestämmelser om sekretess gäller fortfarande i fråga om uppgifter som hänför sig till tiden före ikraftträdandet.

3 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12, 21 och 22 §§ säkerhetsskyddslagen (1996:627) skall ha följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
12 §	
Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller *polisdatalagen (1998:622)*. Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning *eller särskild undersökning i kriminalunderrättelseverksamhet*.	Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller *polisdatalagen (0000.00)*. Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning *eller från en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare*.
21 §	
Utlämnande av uppgifter vid registerkontroll får omfatta	
1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och	
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret, misstankeregistret, *SÄPO-registret och* uppgifter som *annars* behandlas hos Säkerhetspolisen.	2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter *om den kontrollerade* som behandlas hos Säkerhetspolisen.
22 §	
Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som *finns i SÄPO-registret eller annars* behandlas hos Säkerhetspolisen samt de uppgifter om den kon-	Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som behandlas hos Säkerhetspolisen samt de uppgifter om den kontrollerade som finns i belastnings-

trollerade som finns i belastningsregistret och i misstankeregistret om dom eller misstanke om brott som avses i

registret och i misstankeregistret om dom eller misstanke om brott som avses i

– 3 kap. 1, 2, 5 och 6 §§ brottsbalken,
– 4 kap. 1–6 och 8–9 a §§ brottsbalken,
– 6 kap. 1 och 2 §§ brottsbalken,
– 8 kap. 4–6 §§ brottsbalken,
– 9 kap. 3 och 4 §§ brottsbalken,
– 12 kap. 3 § brottsbalken,
– 13 kap. 1–5 b och 7 §§ brottsbalken,
– 16 kap. 1–3, 5, 6 och 8 §§ brottsbalken,
– 17 kap. 1 § brottsbalken,
– 18 kap. 1 och 3–5 §§ brottsbalken,
– 19 kap. brottsbalken,
– 1 och 3 §§ narkotikastrafflagen (1968:64), och
– 9 kap. 1 § vapenlagen (1996:67).

Även uppgift om försök och förberedelse till dessa gärningar får lämnas ut.

Denna lag träder i kraft den 1 juli 2003.

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

Härigenom föreskrivs att 5 § lagen (2000:344) om Schengens informationssystem skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 §	
Registret skall endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.	
Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen (1998:622*) eller annan svensk författning.	Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen (0000:00)* eller annan svensk författning.

Denna lag träder i kraft den 1 juli 2003.

Förteckning över remissinstanserna

Bilaga 3

Efter remiss av betänkandet Behandling av personuppgifter i polisens verksamhet (SOU 2001:92) har remissyttranden avgetts av Riksdagens ombudsmän, Justitiekanslern, Domstolsverket, Riksåklagaren, Ekobrottsmyndigheten, Rikspolisstyrelsen, Registernämnden, Statens kriminaltekniska laboratorium, Kriminalvårdsstyrelsen, Brottsförebyggande rådet, Brottsoffermyndigheten, Datainspektionen, Statskontoret, Statistiska centralbyrån, Försvarsmakten, Socialstyrelsen, Tullverket, Riksrevisionsverket, Riksarkivet, Svea hovrätt, Malmö tingsrätt, Umeå tingsrätt, Kammarrätten i Jönköping, Uppsala universitet, Lunds universitet, Länsstyrelsen i Östergötlands län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Gotlands län, Länsstyrelsen i Skåne län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Örebro län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen Jämtlands län, Länsstyrelsen i Västerbottens län, Kustbevakningen, Riksskatteverket, Ombudsmannen mot diskriminering på grund av sexuell läggning, Sveriges advokatsamfund och Sveriges domareförbund. Riksskatteverket har bifogat yttranden från Skattemyndigheten i Stockholm, Skattemyndigheten i Göteborg och Skattemyndigheten i Malmö.

1 Förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Härigenom föreskrivs följande.

1 kap. Lagens syfte och tillämpningsområde

Lagens syfte

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Lagens tillämpningsområde m.m.

2 § Denna lag gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 2 kap. 4 § andra stycket och 10 § gäller även vid andra myndigheters behandling av uppgifter som har lämnats ut genom direktåtkomst med stöd av denna lag.

Lagen gäller inte vid sådan behandling av personuppgifter som sker enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2008:000) om polisens allmänna spaningsregister. Den gäller inte heller vid insamling av personuppgifter genom allmän kameraövervakning, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning.

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

1. 2 kap. 4 § om personuppgiftsansvar,
2. 2 kap. 5–7 §§ om ändamålen för behandlingen,
3. 2 kap. 11 § om gallring,
4. 3 kap. 1–18 §§ om gemensamt tillgängliga uppgifter,
5. 4 kap. 20–22 §§ om behandling av uppgifter i penningtvättsregister,
6. 5 kap. 2–4 §§ om ändamålen för behandlingen hos Säkerhetspolisen,
7. 5 kap. 6 § om Säkerhetspolisens personuppgiftsansvar,
8. 5 kap. 7 § om gallring hos Säkerhetspolisen, och
9. 5 kap. 8–17 §§ om gemensamt tillgängliga uppgifter hos Säkerhetspolisen.

Vad som sägs i de angivna paragraferna om personuppgifter ska därvid avse uppgifter om juridiska personer.

4 § I 2 kap. finns allmänna bestämmelser om sådan behandling av personuppgifter som omfattas av lagen. För behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även bestämmelserna i 3 kap. För behandling i register med uppgifter om resultat av DNA-analyser, fingeravtrycksregister, signalementsregister eller penningtvättsregister, gäller dock särskilda bestämmelser i 4 kap. i stället för bestämmelserna i 3 kap.

Bestämmelserna i 5 kap. gäller för behandling av personuppgifter i Säkerhetspolisens verksamhet. Vid sådan behandling ska bestämmelserna i 2–4 kap. tillämpas endast i den utsträckning som framgår av 5 kap.

2 kap. Allmänna bestämmelser om personuppgiftsbehandling i polisens brottsbekämpande verksamhet

Förhållandet till personuppgiftslagen

1 § Om inte annat anges i 2 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

2 § När personuppgifter behandlas enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § första stycket a), b) och e)–h) om grundläggande krav på behandling,
4. 22 § om behandling av personnummer,
5. 23 § och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30–32 §§ om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 36 § andra stycket och 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
12. 48 § om skadestånd, och
13. 51 § första stycket, 52 § första stycket och 53 § om överklagande.

Var och en av de myndigheter som avses i 1 kap. 2 § ska utse ett eller flera personuppgiftsombud.

Information enligt 23 § personuppgiftslagen behöver inte lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Tillsyn

3 § Utöver de bestämmelser om tillsyn som avses i 2 § första stycket 11 finns bestämmelser om tillsyn i 1 § lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet.

4 § Rikspolisstyrelsen eller polismyndigheterna är personuppgiftsansvariga för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

En myndighet som har direktåtkomst till uppgifter enligt denna lag ansvarar för att åtkomsten begränsas enligt 10 §.

Ändamål med behandlingen av personuppgifter

5 § Personuppgifter får, om inte annat följer av 6 eller 7 §, behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller beivra brott, eller
3. fullgöra de förpliktelser som följer av internationella åtaganden.

6 § Om personuppgifter behandlas enligt 5 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,
3. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen, eller
4. annan myndighets verksamhet, om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift.

Personuppgifter som behandlas enligt 5 § får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 5 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter och att uppgifter som behandlas i en förundersökning får tillhandahållas konkursförvaltare.

7 § Personuppgifter får alltid behandlas om

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

Behandling av känsliga personuppgifter

8 § Uppgifter om en person får inte behandlas 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.

Trots bestämmelsen i första stycket får uppgifter om en person som behandlas på annan grund kompletteras med uppgifter som avses i första

stycket, om det är absolut nödvändigt för syftet med behandlingen. Uppgifter som avses i första stycket får också behandlas om

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

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

Behandling av uppgifter om resultat av DNA-analyser

9 § Uppgifter om resultat av DNA-analyser får endast behandlas

1. i en förundersökning, eller
2. enligt bestämmelserna i 4 kap. om behandling i DNA-register, utredningsregister och spårregister.

Tillgången till personuppgifter

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

Gallring

11 § Personuppgifter som behandlas automatiserat i ett ärende ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

Utlämnande av uppgifter och uppgiftsskyldighet

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

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

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas

1. till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott, eller
2. till utländsk underrättelse- eller säkerhetstjänst.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.

14 § Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter som har gjorts gemensamt tillgängliga hos polisen lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Första stycket gäller inte uppgifter som behandlas i särskilda register med stöd av 4 kap.

15 § Uppgift om huruvida en person förekommer i register med uppgifter om resultat av DNA-analyser ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Åklagarmyndigheten och Ekobrottsmyndigheten, om den mottagande myndigheten har behov av uppgiften i sin brottsbekämpande verksamhet.

16 § Personuppgifter som behandlas i fingeravtrycks- eller signalementsregister med stöd av 4 kap. 14–19 §§ ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet

17 § Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut även i andra fall än som sägs i 12–16 §§.

3 kap. Gemensamt tillgängliga uppgifter

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. Uppgifter som endast ett fåtal bestämda personer inom polisen har rätt att ta del av anses inte som gemensamt tillgängliga.

Personuppgifter som får göras gemensamt tillgängliga

2 § Endast följande personuppgifter får göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, om han eller hon

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas vara farlig för annans personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra de förpliktelser som följer av internationella åtaganden.

5. Uppgifter som har rapporterats till polisens kommunikationscentraler.

Uppgifter om resultat av DNA-analyser får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Uppgifter som avses i första stycket 4 får göras gemensamt tillgängliga endast om det behövs för att fullgöra den aktuella förpliktelsen.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om huruvida en person är föremål för övervakning får dock göras tillgänglig för flera.

Särskilda upplysningar

3 § Vid behandling enligt 1 § ska personuppgifterna förses med en särskild upplysning om det närmare ändamålet med behandlingen. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska det också lämnas upplysning om detta. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

4 § Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska uppgifterna förses med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

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, om inte detta på grund av särskilda omständigheter är onödigt. Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.

Sökning

5 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Vad som sägs i första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

6 § Vid sökning i gemensamt tillgängliga uppgifter på namn, firma, personnummer, samordningsnummer, organisationsnummer eller andra

liknande identitetsbeteckningar får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är misstänkt för brott eller för brottslig verksamhet som avses i 2 § första stycket 1,
3. övervakas enligt 2 § första stycket 2,
4. har anmält ett brott eller är målsägande i ett ärende som rör ansvar för brott,
5. är vittne eller annars ska höras eller avge yttrande i ett ärende,
6. har gett in eller tillhandahållits en handling, eller
7. är anmäld försvunnen.

7 § Bestämmelsen i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller
2. sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen eller som omfattas av andra stycket 2 har åtkomst till.

Bestämmelsen i 6 § gäller inte heller vid sökning som

1. sker för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, och
2. utförs av särskilt angivna tjänstemän med uppgift att undersöka den brottsliga verksamheten eller övervaka personer enligt 2 § första stycket 2.

Om det finns särskilda skäl får, trots bestämmelsen i 6 §, sökning även ske för att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver, om sökningen utförs av särskilt angivna tjänstemän.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får äga rum med stöd av andra eller tredje stycket.

Utlämnande av uppgifter på medium för automatiserad behandling

8 § Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

Direktåtkomst

9 § Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

10 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Behandling av uppgifter i brottsanmälningar

11 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får uppgifterna inte behandlas i polisens brottsbekämpande verksamhet efter det att det påstådda brottet har preskriberats**.**

Behandling av uppgifter i avslutade förundersökningar

12 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år sedan domen, eller det beslut som meddelades med anledning av talan, vann laga kraft.

Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter åklagarens eller förundersökningsledarens beslut. Om det i samband med beslutet anges att brottet, trots nedläggningsbeslutet, kan komma att bli föremål för lagföring, får dock behandling ske även senare fram till dess att brottet har preskriberats.

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

13 § Trots bestämmelserna i 12 § får personuppgifter i en förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken behandlas i polisens brottsbekämpande verksamhet, om det behövs för att återuppta förundersökningen eller utredningen eller för en prövning enligt 58 eller 59 kap. rättegångsbalken. Om det finns särskilda skäl, får uppgifterna även behandlas, om det behövs för en utredning som avser brott, för vilket är föreskrivet fängelse i fyra år eller däröver, eller för en undersökning av brottslig verksamhet som innefattar sådant brott.

14 § Om en förundersökning mot en person har lagts ned på grund av bristande bevisning, om åtal har lagts ned eller om frikännande dom, som har vunnit laga kraft, har meddelats, får en uppgift om att personen är misstänkt för brott inte längre vara sökbar, om inte förundersökningsledaren har beslutat att återuppta förundersökningen eller fråga är om prövning enligt 58 eller 59 kap. rättegångsbalken.

15 § Bestämmelserna i 11–14 §§ hindrar inte att personuppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken arkiveras och gallras enligt bestämmelserna i arkivlagen (1990:782). För användningen av arkiverade uppgifter i polisens brottsbekämpande verksamhet gäller dock de begränsningar som anges i 11–14 §§**.**

Gallring

16 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras enligt bestämmelserna i andra–sjätte styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om den person som uppgiften avser inte är eller varit misstänkt, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende den övervakade personen gjordes. Om en uppgift inte avser den övervakade personen, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats med stöd av 2 § första stycket 4 ska gallras senast ett år efter det att ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som har behandlats med stöd av 2 § första stycket 5 ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i andra och tredje styckena.

17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och
2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 gäller vad som sägs i 11–15 §§.

18 § Vad som föreskrivs i 11–16 §§ hindrar inte att regeringen meddelar föreskrifter om att uppgifter i vissa särskilda fall får behandlas och bevaras under längre tid än vad som anges där.

4 kap. Register

Register med uppgifter om resultat av DNA-analyser

Ändamål m.m.

1 § Med DNA-analys förstås varje förfarande som kan användas för analys av deoxyribonukleinsyra.

2 § Rikspolisstyrelsen får föra register över uppgifter om resultat av DNA-analyser i enlighet med 3–13 §§ (DNA-register, utredningsregister och spårregister). Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av avlidna personer.

DNA-register

3 § Ett DNA-register får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller
2. har godkänt ett strafföreläggande som avser villkorlig dom.

4 § Registreringen av resultatet av en DNA-analys ska begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser.

Utredningsregister

5 § Ett utredningsregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket fängelse kan följa.

Vad som anges i 4 § gäller också vid registrering i utredningsregistret.

Spårregister

6 § Ett spårregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver uppgifter om analysresultat får spårregistret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts.

7 § Uppgifter i ett spårregister får endast jämföras med analysresultat

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

8 § Uppgifter i DNA-registret ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i utredningsregistret ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter i spårregistret ska gallras senast trettio år efter registreringen.

Särskilda bestämmelser om prov för DNA-analys

9 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys, får provet inte användas för något annat ändamål än det för vilket det togs.

10 § Ett prov för DNA-analys som har tagits med stöd av bestämmelserna i 28 kap. 12–12 b §§ rättegångsbalken ska förstöras senast sex månader efter det att provet togs.

Om uppgifterna i utredningsregistret ska gallras vid en tidigare tidpunkt enligt 8 §, ska även det prov som avser den registrerade förstöras senast vid samma tidpunkt.

Om provet har tagits från någon som inte är skäligen misstänkt för brott, ska provet förstöras så snart målet eller ärendet slutligt har avgjorts.

Utlämnande av uppgifter på medium för automatiserad behandling

11 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter om resultat av DNA-analyser.

Direktåtkomst

12 § Statens kriminaltekniska laboratorium, polismyndigheter, Ekobrottsmyndigheten och Åklagarmyndigheten får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

13 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

Ändamål

14 § Rikspolisstyrelsen får föra fingeravtrycks- eller signalementsregister i enlighet med 15–19 §§. Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av okända personer.

Innehåll

15 § Ett fingeravtrycks- eller signalementsregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I ett sådant register får endast antecknas uppgifter om

1. fingeravtryck,
2. signalement,
3. identifieringsuppgifter,
4. ärendenummer, och
5. brottskoder.

Fingeravtrycks- eller signalementsregister får inte innehålla uppgifter som har lämnats av en person under femton år enligt 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Gallring

16 § Uppgifter i ett fingeravtrycks- eller signalementsregister om en misstänkt person ska gallras senast

1. tio år efter registreringen, om denna skett på grund av misstanke om brott för vilket det inte föreskrivs strängare straff än fängelse i två år,
2. femton år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i två år men inte strängare straff än fängelse i åtta år,
3. tjugofem år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i åtta år,
4. tre månader efter det att åtal mot personen har lagts ned eller efter att personen genom lagakraftvunnen dom har frikänts, eller
5. tre månader efter det att en förundersökning mot personen har lagts ned.

Om en person blir misstänkt för ett nytt brott före utgången av den tid som anges i första stycket 1, 2 eller 3 får de uppgifter som finns registrerade om personen bevaras till dess att den senare registreringen avseende personen ska gallras enligt första stycket.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll ska gallras när uppgifterna inte längre behövs för ändamålet med behandlingen eller enligt föreskrifter som regeringen meddelar.

17 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter i ett fingeravtrycks- eller signalementsregister.

Direktåtkomst

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i ett fingeravtrycks- eller signalementsregister.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

19 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till ett fingeravtrycks- eller signalementsregister i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

Penningtvättsregister

Ändamål m.m.

20 § Rikspolisstyrelsen får behandla uppgifter i penningtvättsregister om det behövs för att förebygga, förhindra eller upptäcka

1. brottslig verksamhet där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller
2. brottslig verksamhet som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

I ett sådant register får endast behandlas uppgifter som kan antas ha samband med sådan misstänkt brottslig verksamhet som avses i första stycket 1 och 2, uppgifter som har rapporterats till myndigheten med stöd av bestämmelser i lag eller annan författning och uppgifter som har lämnats av en utländsk myndighet som ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i första stycket 1 och 2 i det landet.

Gallring

21 § Personuppgifter i ett penningtvättsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Första stycket gäller inte om regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att uppgifter ska bevaras för historiska, statistiska eller vetenskapliga ändamål.

22 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för uppgifter i ett penningtvättsregister.

5 kap. Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

Allmänna bestämmelser

1 § Detta kapitel innehåller bestämmelser om behandling av personuppgifter hos Säkerhetspolisen i dess brottsbekämpande verksamhet.

Ändamål

2 § I Säkerhetspolisens brottsbekämpande verksamhet får, om inte annat följer av 3 eller 4 §, personuppgifter behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
   a) brott mot rikets säkerhet,
   b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,
   c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., eller
   d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,
2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra bevaknings- och säkerhetsarbete avseende personskydd,
4. fullgöra de uppgifter som följer av säkerhetsskyddslagen (1996:627),
5. fullgöra de förpliktelser som följer av internationella åtaganden, eller
6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

3 § Om personuppgifter behandlas enligt 2 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller
3. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation.

Personuppgifter som behandlas enligt 2 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 2 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter.

4 § Bestämmelserna i 2 kap. 7 § om diarieföring av personuppgifter m.m. gäller även för behandling av personuppgifter hos Säkerhetspolisen.

Tillämpliga bestämmelser i 2 kap.

5 § Följande bestämmelser i 2 kap. ska tillämpas vid behandling av personuppgifter hos Säkerhetspolisen:

1. 1 och 2 §§ om förhållandet till personuppgiftslagen,
2. 3 § om tillsyn,
3. 8 § om behandling av känsliga personuppgifter,
4. 9 § om behandling av uppgifter om resultatet av DNA-analyser,
5. 10 § om tillgången till uppgifter, och
6. 12, 13 och 17 §§ om utlämnande av uppgifter.

Personuppgiftsansvar

6 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

Gallring

7 § Personuppgifter som behandlas automatiserat i ett ärende hos Säkerhetspolisen ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

Gemensamt tillgängliga uppgifter

8 § Om det behövs för de ändamål som anges i 2 §, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet. Uppgifter om resultat av DNA-analyser får dock inte göras gemensamt tillgängliga. Uppgifter som endast ett fåtal bestämda personer hos Säkerhetspolisen har rätt att ta del av anses inte som gemensamt tillgängliga.

Bestämmelserna i 9–17 §§ gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

9 § Vid behandling enligt 8 § ska personuppgifterna förses med en särskild upplysning om det närmare ändamålet med behandlingen. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

10 § Om uppgifter, som behandlas enligt 8 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska de förses med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

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. Upplysning behöver dock inte lämnas, om det på grund av särskilda omständigheter är onödigt. Upplysning 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 och analysen befinner sig i ett inledande skede.

Sökning

11 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som anges i 2 §.

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

12 § Vid sökning i gemensamt tillgängliga uppgifter får endast följande uppgifter tas fram:

1. identifieringsuppgifter,
2. uppgifter om grunden för registreringen, och
3. hänvisning till de ärenden där uppgifter om personen behandlas.

13 § Bestämmelsen i 12 § gäller inte vid sökning

1. i en viss handling eller i ett visst ärende, eller
2. i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får ske enligt första stycket.

14 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling ska tillämpas även vid utlämnande av uppgifter som behandlas hos Säkerhetspolisen.

Behandling av uppgifter i avslutade förundersökningar m.m.

15 § Bestämmelserna i 3 kap. 11–15 §§ om behandling av uppgifter i avslutade förundersökningar m.m. ska tillämpas även vid behandling av personuppgifter hos Säkerhetspolisen.

Gallring

16 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en sådan uppgiftssamling som avses i 10 § andra stycket 1 ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Säkerhetspolisen får besluta att personuppgifter får behandlas längre tid än vad som sägs i första och andra styckena, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i andra stycket, senast vid utgången av det tredje kalenderåret efter beslutet.

17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och
2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 ska i stället 3 kap. 11–15 §§ tillämpas.

---

1. Denna lag träder i kraft den 1 januari 2009, då polisdatalagen (1998:622) upphör att gälla.

2. I fråga om behandling av personuppgifter i en särskild undersökning enligt 14 § första stycket 1 polisdatalagen (1998:622) som har beslutats före ikraftträdandet av denna lag gäller bestämmelserna i polisdatalagen i stället för bestämmelserna i denna lag till utgången av år 2010.

3. För de personregister som har förts med stöd av punkten 2 i övergångsbestämmelserna till polisdatalagen (1998:622) gäller bestämmelserna i datalagen (1973:289) i stället för bestämmelserna i denna lag till utgången av år 2010. Bestämmelserna i 2 kap. 12, 13 och 17 §§ denna

lag ska dock tillämpas på uppgifterna i registren från lagens ikraftträdande.

Vad som sägs i första stycket gäller inte fingeravtrycksregistret, signalements- och känneteckensregistret och det allmänna spaningsregistret.

4. Datainspektionens tillstånd att föra sådana register som avses i punkten 3 andra stycket upphör att gälla vid ikraftträdandet av denna lag.

Datainspektionens tillstånd att föra övriga register som avses i punkten 3 upphör att gälla vid utgången av år 2010 eller vid den tidigare tidpunkt då den personuppgiftsansvarige avanmäler registret hos inspektionen.

5. Bestämmelserna om särskilda upplysningar i 3 kap. 3 och 4 §§ behöver inte tillämpas förrän den 1 januari 2011 i fråga om uppgifter som har samlats in före ikraftträdandet.

6. Bestämmelserna om gallring och om behandling av uppgifter i brottsanmälningar och avslutade förundersökningar i 3 kap. 11–17 och 5 kap. 15 §§ ska inte tillämpas förrän den 1 januari 2011 i fråga om uppgifter som har samlats in före ikraftträdandet. I stället ska motsvarande bestämmelser i polisdatalagen (1998:622) tillämpas. För uppgifter i ett register som har avanmälts enligt punkten 4 gäller dock bestämmelserna i denna lag.

Härigenom föreskrivs följande.

Allmänt spaningsregister

1 § Rikspolisstyrelsen får med hjälp av automatiserad behandling föra ett allmänt spaningsregister.

Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret. En myndighet som har direktåtkomst enligt denna lag ansvarar för att åtkomsten begränsas enligt 11 §.

Ändamål

2 § Det allmänna spaningsregistret ska ha till ändamål att underlätta tillgången till personuppgifter som behövs för spaning i polisens brottsbekämpande verksamhet.

Vilka personuppgifter som får behandlas

3 § I det allmänna spaningsregistret får behandlas uppgifter som kan hänföras till en enskild person, om

1. den som uppgiften avser kan misstänkas för att ha begått ett brott som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

4 § I registret får behandlas uppgifter som kan hänföras till en enskild person som inte kan misstänkas för brott, om uppgiften

1. har samband med en person som har registrerats enligt 3 §, och
2. är av särskild betydelse för polisens spaningsverksamhet.

5 § Utöver de uppgifter som får behandlas enligt 3 och 4 §§ får uppgifter behandlas om en juridisk person, ett transportmedel eller annat föremål som kan hänföras till en enskild person, om

1. uppgiften kan antas ha samband med ett brott som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

Innehåll

6 § Det allmänna spaningsregistret ska innehålla uppgifter om

1. grunden för att en person registreras enligt 3 § eller att en juridisk person, ett transportmedel eller föremål enligt 5 § förs in i registret och omständigheterna i samband med registreringen,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än sådana som avses i 1 tillförs registret,
3. den behandlade uppgiftens ursprung, och
4. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

7 § Det allmänna spaningsregistret får, utöver vad som anges i 6 §, endast innehålla följande uppgifter om en person som har registrerats enligt 3 §:

1. uppgift som är ägnad att identifiera personen, dock inte uppgifter om resultat av DNA-analyser eller fingeravtryck,
2. uppgift om vistelseadress,
3. uppgift om verkställighet av påföljd för brott,
4. uppgift om att personen är eftersökt i samband med brott,
5. uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
6. uppgift om att personen är föremål för sådan övervakning som avses i 3 kap. 2 § första stycket 2 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
7. uppgift om anknytning till juridisk person,
8. uppgift om anknytning till andra personer som har registrerats enligt 3 § och som kan antas tillhöra samma gruppering som den registrerade,
9. uppgift om att personen har något speciellt tillvägagångssätt, och
10. ärendenummer.

8 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får registreras i det allmänna spaningsregistret och om förfarandet vid registreringen.

Särskilda upplysningar

9 § Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte misstänks för brott ska förses med en särskild upplysning om detta. Detsamma gäller uppgifter om en juridisk person eller ett transportmedel som indirekt kan hänföras till en sådan person. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

Registrering av känsliga personuppgifter

10 § Uppgifter om en person får inte registreras i det allmänna spaningsregistret 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.

Trots bestämmelsen i första stycket får uppgifter om en person som registreras på annan grund kompletteras med sådana uppgifter som avses i första stycket om det är absolut nödvändigt för syftet med registreringen.

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

Tillgången till personuppgifter

11 § Tillgången till personuppgifter i det allmänna spaningsregistret ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

12 § Uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv får inte användas som sökbegrepp vid sökning i det allmänna spaningsregistret. Detta hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

13 § Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara.

Utlämnande av uppgifter och uppgiftsskyldighet

14 § Personuppgifter i det allmänna spaningsregistret som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

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

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.

16 § Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter i det allmänna spaningsregistret lämnas till

1. polismyndighet, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet, eller
2. polismyndighet, om myndigheten har behov av uppgifterna i annan verksamhet än den brottsbekämpande verksamheten och det finns särskilda skäl för att lämna ut dem.

Regeringen meddelar föreskrifter om att uppgifter får lämnas ut till andra myndigheter än de som anges i första stycket.

Utlämnande av uppgifter på medium för automatiserad behandling

17 § Endast enstaka personuppgifter i det allmänna spaningsregistret får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall har beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket och Kustbevakningen får medges direktåtkomst till det allmänna spaningsregistret.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Gallring

19 § Uppgifter i det allmänna spaningsregistret om en person som har registrerats enligt 3 § ska gallras senast tre år efter det att uppgiften om misstanke om brott registrerades. Om uppgiften avser misstanke om brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter registreringen.

Om en ytterligare uppgift om personen förs in i registret, behöver uppgifterna om den registrerade personen inte gallras förrän

1. fem år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. tre år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om annat brott än i 1, eller
3. ett år från det att den nya uppgiften fördes in i registret, om uppgiften inte avser misstanke om brott.

Den tid under vilken en person som har registrerats enligt 3 § avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i första och andra styckena.

Uppgifter om en person som avses i 4 § ska gallras senast när uppgifterna om den person som har registrerats enligt 3 § och som uppgifterna har samband med gallras.

20 § Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats enligt 5 § ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter det att den senaste uppgiften infördes.

21 § Vad som föreskrivs i 19 och 20 §§ hindrar inte att regeringen eller den myndighet som regeringen bestämmer

1. meddelar föreskrifter om att uppgifter gallras vid en tidigare tidpunkt, eller bevaras för historiska, statistiska eller vetenskapliga ändamål, eller
2. i ett enskilt fall beslutar att en uppgift ska bevaras om det finns synnerliga skäl för det.

Ett beslut enligt första stycket 2 ska omprövas varje år.

22 § Bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen.

Denna lag träder i kraft den 1 januari 2009 och gäller till och med den 31 december 2014.

Härigenom föreskrivs att 28 kap. 12 a och 12 b §§ rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
28 kap.	
12 a §[6]	
Kroppsbesiktning genom tagande av salivprov får ske på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det DNA-register eller det utredningsregister som förs enligt *polisdatalagen (1998:622)*.	Kroppsbesiktning genom tagande av salivprov får ske på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det DNA-register eller det utredningsregister som förs enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.*
12 b §[7]	
Kroppsbesiktning genom tagande av salivprov får ske på annan än den som skäligen kan misstänkas för ett brott, om	Kroppsbesiktning genom tagande av salivprov får ske på annan än den som skäligen kan misstänkas för ett brott, om
1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och	1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och
2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.	2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.
Analysresultatet får inte jämföras med de uppgifter som finns registrerade i register som förs enligt *polisdatalagen (1998:622)* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.	Analysresultatet får inte jämföras med de uppgifter som finns registrerade i register som förs enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.
Första stycket gäller inte den som är under 15 år.	Första stycket gäller inte den som är under 15 år.

[6] Senaste lydelse 2005:878.
[7] Senaste lydelse 2005:878.

Denna lag träder i kraft den 1 januari 2009.

Härigenom föreskrivs att 5 kap. 1 och 7 §§, 7 kap. 41 § och 9 kap. 17 § sekretesslagen (1980:100) [1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 kap.

1 § [2]

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,

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

3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,

4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, eller

5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till *sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott* gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av upp-

För uppgift som hänför sig till *verksamhet hos polisen enligt 2 kap. 5 § 1 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller till verksamhet hos Säkerhetspolisen enligt 5 kap. 2 § 1 samma lag* gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av upp-

[1] Lagen omtryckt 1992:1474.
[2] Senaste lydelse 2006:697.

het som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

gifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndigheten i konkurs och hos Kronofogdemyndigheten för uppgift som angår misstanke om brott.

Utan hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av

1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,
2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid Rikspolisstyrelsens säkerhetsavdelning, eller
3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

7 §[3]

Sekretess gäller i verksamhet som avser rättsligt samarbete på begäran av annan stat eller mellanfolklig domstol för uppgift som hänför sig till

1. utredning enligt bestämmelserna om förundersökning i brottmål, eller
2. angelägenhet som angår tvångsmedel,

om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622)* och lagen om Schengens informationssystem.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* och lagen om Schengens informationssystem.

[3] Senaste lydelse 2003:1161.

I fråga om uppgift i allmän handling gäller sekretessen i högst fyrtio år.

7 kap.

41 §[4]

Sekretess gäller hos polismyndighet och åklagarmyndighet, samt hos Rikspolisstyrelsen, Tullverket, Kustbevakningen och Migrationsverket, för uppgift om enskilds personliga förhållanden i en angelägenhet som avser en framställning enligt 3 § lagen (2000:344) om Schengens informationssystem

1. om omhändertagande av en person som har efterlysts för överlämnande eller utlämning,

2. om att en person *skall* nekas tillträde till eller uppehållstillstånd i Schengenstaterna (spärrlista),

2. om att en person *ska* nekas tillträde till eller uppehållstillstånd i Schengenstaterna (spärrlista),

3. om tillfälligt omhändertagande av en person med hänsyn till dennes eller någon annans säkerhet, samt

4. om dold övervakning eller särskilda kontrollåtgärder,

om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon honom närstående lider men.

Sekretess gäller hos myndighet som prövar ansökningar om visering och uppehållstillstånd för uppgift om enskilds personliga förhållanden i en angelägenhet som avser en sådan framställning som avses i första stycket 2 under samma förutsättningar som anges i första stycket.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622)* och lagen (2000:344) om Schengens informationssystem.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* och lagen (2000:344) om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

9 kap.

17 §[5]

Sekretess gäller för uppgift om enskilds personliga och ekonomiska förhållanden, om inte annat följer av 18 §

1. i utredning enligt bestämmelserna om förundersökning i brottmål,

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

3. i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. i åklagarmyndighets, polismyndighets, Skatteverkets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

[4] Senaste lydelse 2003:1161.
[5] Senaste lydelse 2006:697.

5. i Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller polismyndighet i brottmål,	
6. i register som förs av Rikspolisstyrelsen enligt *polisdatalagen (1998:622)* eller som annars behandlas där med stöd av samma lag,	6. i register som förs av Rikspolisstyrelsen enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller som annars behandlas där med stöd av samma lag,
7. i register som förs enligt lagen (1998:621) om misstankeregister,	
	8. i det register som förs enligt lagen (2008:000) om polisens allmänna spaningsregister,
8. i register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,	*9.* i register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,
9. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,	*10***.** i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,
10. i register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas med stöd av samma lag,	*11.* i register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas med stöd av samma lag,

om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men.

Sekretess enligt första stycket 2 gäller hos domstol i dess rättsskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till den enskilde 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 annat allvarligt men om uppgiften röjs. Av 12 kap. 2 § andra stycket framgår att även sekretessen enligt första stycket 1 är begränsad hos domstol.

Sekretess enligt första stycket gäller hos tillsynsmyndigheten i konkurs för uppgift som angår misstanke om brott.

Sekretess gäller i verksamhet, som avses i första stycket, för anmälan eller utsaga från enskild, om det kan antas att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs.

Utan hinder av sekretessen får en skadelidande, eller den som den skadelidande överlåtit sin rätt till, ta del av en uppgift

1. i en nedlagd förundersökning eller i en förundersökning som	1. i en nedlagd förundersökning eller i en förundersökning som

avslutats med ett beslut om att åtal inte *skall* väckas,	avslutats med ett beslut om att åtal inte *ska* väckas,

2. i en annan brottsutredning som utförts enligt bestämmelserna i 23 kap. rättegångsbalken och som avslutats på annat sätt än med beslut att väcka åtal, med strafföreläggande eller med föreläggande av ordningsbot, eller

3. i en avslutad utredning enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

om den skadelidande, eller den som den skadelidande överlåtit sin rätt till, behöver uppgiften för att kunna få ett anspråk på skadestånd eller på bättre rätt till viss egendom tillgodosett och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående till honom eller henne att den inte lämnas ut.

Utan hinder av sekretessen får en uppgift också lämnas ut

1. till enskild enligt vad som föreskrivs i den särskilda lagstiftningen om unga lagöverträdare,

2. till enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) samt i förordning som har stöd i den lagen,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen (1998:622)*, lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar,	3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* samt i förordningar som har stöd i dessa lagar,

4. till enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

Utan hinder av sekretessen får polisen på begäran av den som lidit person- eller sakskada vid en trafikolycka lämna uppgift om identiteten hos en trafikant som haft del i olyckan.

Utan hinder av sekretessen enligt första stycket 1 får uppgift lämnas till konkursförvaltare, om uppgiften kan antas ha betydelse för konkursutredningen.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i första stycket 1–4 eller 6 eller motsvarande verksamhet enligt äldre bestämmelser, om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 januari 2009.

5 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12, 21 och 22 §§ 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 misstankeregister eller polisdatalagen (1998:622). Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild undersökning i kriminalunderrättelseverksamhet.*	Med registerkontroll avses *kontroll av om det förekommer uppgifter om en person i register som förs av polisen eller om sådana uppgifter annars behandlas där i den brottsbekämpande verksamheten.* *Vid en registerkontroll ska uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister. Vidare ska uppgifter hämtas som Säkerhetspolisen behandlar med stöd av 5 kap. lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.* *Uppgifter får också hämtas från register som omfattas av 4 kap. lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller lagen (2008:000) om polisens allmänna spaningsregister. Vidare får uppgifter hämtas som polisen i övrigt behandlar med stöd av 2 kap. 5 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, om uppgifterna har gjorts gemensamt tillgängliga.* *Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av registerkontrollen.*

[1] Senaste lydelse 1998:625.

21 §[2]

Utlämnande av uppgifter vid registerkontroll får omfatta

1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och

2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret, misstankeregistret, *SÄPO-registret och* uppgifter som *annars* behandlas hos Säkerhetspolisen.

2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.

22 §[3]

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret, misstankeregistret, *SÄPO-registret och* uppgifter som *annars* behandlas hos Säkerhetspolisen.

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.

Denna lag träder i kraft den 1 januari 2009.

[2] Senaste lydelse 1998:625.
[3] Senaste lydelse 2006:347.

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

Härigenom föreskrivs att 2 och 6 §§ lagen (1998:620) om belastningsregister ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §[1]	
Belastningsregistret *skall* föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos	Belastningsregistret *ska* föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos
1. *polis-, skatte- och tullmyndigheter* för att förebygga, upptäcka och utreda brott,	1. *polismyndigheter, Skatteverket, Tullverket* och *Kustbevakningen* för att förebygga, upptäcka och utreda brott,
2. åklagarmyndigheter för beslut om förundersökning och åtal samt för utfärdande av strafföreläggande,	
3. allmänna domstolar för straffmätning och val av påföljd och	
4. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.	
Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.	
6 §[2]	
Personuppgifter ur belastningsregistret *skall* lämnas ut om det begärs av	Personuppgifter ur belastningsregistret *ska* lämnas ut om det begärs av
1. Riksdagens ombudsmän, Justitiekanslern eller Datainspektionen för deras tillsynsverksamhet,	
2. *polis-, skatte-, tull- eller* åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,	2. *polismyndighet, Skatteverket, Tullverket, Kustbevakningen,* åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,
3. förvaltningsdomstol för prövning enligt 2 § första stycket 4 eller	
4. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.	
Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.	

Denna lag träder i kraft den 1 januari 2009.

[1] Senaste lydelse 1999:91.
[2] Senaste lydelse 1999:91.

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

Härigenom föreskrivs att 2 och 5 §§ lagen (1998:621) om misstankeregister ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §[1]	
Misstankeregistret *skall* föras för att underlätta tillgången till sådana uppgifter om skälig misstanke om brott som behövs i verksamhet hos	Misstankeregistret *ska* föras för att underlätta tillgången till sådana uppgifter om skälig misstanke om brott som behövs i verksamhet hos
1. *polis-, skatte-* och *tullmyndigheter* för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott,	1. *polismyndigheter, Skatteverket, Tullverket* och *Kustbevakningen* för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal och

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

Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.

5 §[2]	
Uppgifter ur misstankeregistret *skall* lämnas ut om det begärs av	Uppgifter ur misstankeregistret *ska* lämnas ut om det begärs av
1. *polis-, skatte-, tull- eller* åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,	1. *polismyndighet, Skatteverket, Tullverket, Kustbevakningen,* åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,

2. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.

Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.

Att uppgifter får lämnas ut i vissa andra fall framgår av 14 kap. sekretesslagen (1980:100).

Denna lag träder i kraft den 1 januari 2009.

[1] Senaste lydelse 1999:92.
[2] Senaste lydelse 1999:92.

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

Härigenom föreskrivs att 5 § lagen (2003:344) om Schengens informationssystem ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §
Registret *skall* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.	Registret *ska* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.
Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen (1998:622)* eller annan svensk författning.	Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller annan svensk författning.

Denna lag träder i kraft den 1 januari 2009.

9 Förslag till lag om ändring i lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1 § lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt proposition 2006/07:133	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden (nämnden) *skall* utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.	Säkerhets- och integritetsskyddsnämnden (nämnden) *ska* utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.
Nämnden *skall* även utöva tillsyn över *Säkerhetspolisens* behandling av uppgifter *enligt polisdatalagen (1998:622), särskilt med avseende på 5 § den lagen.*	Nämnden *ska* även utöva tillsyn över *polisens* behandling av uppgifter *enligt lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lagen (2008:000) om polisens allmänna spaningsregister. Tillsynen ska särskilt avse behandlingen av sådana känsliga personuppgifter som avses i 2 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och 10 § lagen om polisens allmänna spaningsregister.*
Tillsynen *skall* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.	Tillsynen *ska* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Denna lag träder i kraft den 1 januari 2009.

Förteckning över remissinstanserna

Efter remiss av departementspromemorian Behandling av personuppgifter i polisens brottsbekämpande verksamhet (Ds 2007:43) har yttranden avgetts av Riksdagens ombudsmän, Riksrevisionen, Justitiekanslern, Domstolsverket, Svea hovrätt, Kammarrätten i Stockholm, Länsrätten i Stockholms län, Länsrätten i Östergötlands län, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Statens kriminaltekniska laboratorium, Kriminalvården, Brottsförebyggande rådet, Brottsoffermyndigheten, Försvarsmakten, Kustbevakningen, Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Datainspektionen, Statskontoret, Länsstyrelsen i Stockholms län, Juridiska fakulteten vid Uppsala universitet, Juridiska fakulteten vid Lunds universitet, Riksarkivet, Sveriges advokatsamfund, Svenska Journalistförbundet, Sveriges Akademikers Centralorganisation (SACO), Svenska polisförbundet, Sveriges Kommuner och Landsting och Tull-Kust.

Facket för Service och Kommunikation (SEKO), ST-polisväsendet, Svenska avdelningen av internationella Juristkommissionen, Svenska Helsingforskommittén för Mänskliga Rättigheter, Sveriges Domareförbund och Tidningsutgivarna har beretts tillfälle att lämna synpunkter men inte inkommit med något yttrande.

Polisens register

Register som regleras särskilt i polisdatalagen

Kriminalunderrättelseregister m.m.

Med underrättelseverksamhet förstås i polisdatalagen (1998:622) den polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken. Med kriminalunderrättelseverksamhet avses annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen. För SÄPO-registret innehåller lagen särskilda bestämmelser (se nedan). Bestämmelser om kriminalunderrättelseverksamhet finns i 14–21 §§ polisdatalagen.

Personuppgifter får behandlas i kriminalunderrättelseregister. Ett kriminalunderrättelseregister får föras för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslig verksamhet eller för att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet. Kriminalunderrättelseregister får föras av Rikspolisstyrelsen eller av en polismyndighet. Den myndighet som för registret är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Ett kriminalunderrättelseregister får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet har utövats eller kan komma att utövas. Med allvarlig brottslig verksamhet menas enligt 3 § polisdatalagen verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver. Det krävs vidare att den person som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva den allvarliga brottsliga verksamheten. Uppgifter om transportmedel eller varor som kan antas ha samband med allvarlig brottslig verksamhet eller om hjälpmedel som kan ha använts i samband med sådan verksamhet får dock registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna ska då förses med upplysning om att det inte finns några misstankar mot denne.

I polisdatalagen anges vilka uppgifter som får finnas i ett kriminalunderrättelseregister. Ett sådant register får endast innehålla

– upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet,
– identifieringsuppgifter,
– uppgifter om särskilda bestående fysiska kännetecken,
– de omständigheter och händelser som ger anledning att anta att den registrerade utövat eller kan komma att utöva allvarlig brottslig verksamhet,
– uppgifter om varor, brottshjälpmedel och transportmedel,
– ärendenummer, och
– hänvisning till en särskild undersökning där uppgifter om den registrerade behandlas och till register som förs av polis-, skatte- eller tullmyndighet i vilket uppgifter om den registrerade förekommer.

Uppgifter i ett kriminalunderrättelseregister om en registrerad person ska gallras senast tre år efter det att uppgifter om att denne skäligen kan misstänkas för att ha utövat eller komma att utöva allvarlig brottslig verksamhet senast infördes. Om det dessförinnan har inletts en särskild undersökning som rör den registrerade personen, får uppgifterna stå kvar tills undersökningen har avslutats. Regeringen, eller den myndighet som regeringen bestämmer, får vidare meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål.

Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten får enligt 9 § polisdataförordningen (1999:81) ha direkt åtkomst till kriminalunderrättelseregistren. Åtkomsten till registren ska förbehållas de personer som på grund av sina arbetsuppgifter behöver tillgång till information om sådana uppgifter som behandlas i registren. Vid Ekobrottsmyndigheten får endast polisman och annan person som deltar i polisiärt arbete, med undantag för åklagare, ha direktåtkomst till kriminalunderrättelseregistren.

Uppgifter ur ett kriminalunderrättelseregister får enligt 10 § polisdataförordningen lämnas ut till Kustbevakningen, Tullverket eller Skatteverket. Utlämnande får dock endast ske om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

I kriminalunderrättelseverksamhet får vidare automatiserad behandling av personuppgifter förekomma i s.k. särskilda undersökningar. Sådana får inledas efter särskilt beslut om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas. Undersökningarna görs i syfte att ge underlag för beslut om förundersökning eller för beslut om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. I särskilda undersökningar får även uppgifter om icke misstänkta personer behandlas, men uppgifterna måste förses med upplysning om att personen inte är misstänkt. Som exempel på en särskild undersökning kan nämnas den undersökning som gjordes inför Europeiska rådets möte i Göteborg den 14–16 juni 2001 vid Polismyndigheten i Västra Götaland (SOU 2002:122 s. 258 f).

Det centrala kriminalunderrättelseregistret

Det centrala kriminalunderrättelseregistret utgör en nationell, gemensam databas som polismyndigheterna och Rikspolisstyrelsen har tillgång till. De enheter som bedriver kriminalunderrättelseverksamhet har därigenom ett system för att lagra uppgifter för att kunna återfinna handlingar. Endast sådana befattningshavare som är knutna till enheter eller rotlar som sysslar med kriminalunderrättelseverksamhet har behörighet att behandla uppgifter i registret.

Innehållet i det centrala kriminalunderrättelseregistret består av underrättelseinformation som kommit in till en enhet som bedriver underrättelseverksamhet eller Rikspolisstyrelsen från polismän, från allmänheten, andra myndigheter eller internationella organisationer. Informationen kan också ha kommit fram vid det interna arbetet på roteln eller genom underrättelser från något annat land.

I det centrala kriminalunderrättelseregistret finns personuppgifter som avser personer vilka skäligen kan misstänkas för att de kan komma att utöva, utövar eller har utövat allvarlig brottslig verksamhet. Misstankarna behöver inte avse konkreta brott. Registret innehåller även uppgifter om transportmedel och hjälpmedel som förekommer i allvarlig brottslig verksamhet. I de fall där dessa uppgifter kan hänföras till en person som det inte föreligger någon misstanke mot, förses uppgifterna med en upplysning om detta.

Från det centrala kriminalunderrättelseregistret hämtas särskilt utvalda uppgifter för registrering i Europols informationssystem. Detta tillhandahålls av Europol för gemensam användning av medlemsstaternas nationella enheter och Europol. Systemet tillförs uppgifter dels av medlemsstaternas nationella enheter, dels av Europol. I Sverige är Rikspolisstyrelsen personuppgiftsansvarig för de personuppgifter som styrelsen behandlar i systemet. I artikel 8 i rådsbeslutet om inrättandet av den Europeiska Polisbyrån, Europol, finns bestämmelser om medlemsstaternas nationella enheter och deras skyldighet att förse Europol med information. I artikel 12 i rådsbeslutet regleras vilka uppgifter som får registreras i Europols informationssystem.

Register med uppgifter om DNA-analyser

Resultatet av prov som tagits för DNA-analys med stöd av bestämmelserna om kroppsbesiktning i 28 kap. rättegångsbalken får under vissa förutsättningar registreras i register som förs med stöd av polisdatalagen. Bestämmelser om dessa register finns i 22–28 §§ polisdatalagen.

Med stöd av polisdatalagen för Rikspolisstyrelsen tre olika register; DNA-register, utredningsregister och spårregister. DNA-registret innehåller DNA-profiler från personer som dömts till annan påföljd än enbart böter. Utredningsregister innehåller DNA-profiler från personer som är skäligen misstänkta för brott på vilket fängelse kan följa. Spårregister innehåller DNA-profiler från spår som påträffats under utredning av ett brott och som inte kan hänföras till en identifierbar person. Rikspolisstyrelsen är personuppgiftsansvarig för samtliga register. Registren förs hos Statens kriminaltekniska laboratorium i egenskap av personuppgiftsbiträde åt Rikspolisstyrelsen.

Uppgifter om en person i DNA-register ska gallras när de inte längre behövs och senast när uppgifterna om den registrerade har gallrats ur belastningsregistret. Uppgifterna i utredningsregister ska gallras när förundersökning eller åtal läggs ned, åtal ogillas eller åtal bifalls men påföljden bestäms till enbart böter. Uppgifter i spårregister ska gallras när de inte längre behövs och senast trettio år efter registreringen.

Statens kriminaltekniska laboratorium, polismyndigheter och Åklagarmyndigheten får enligt 11 § polisdataförordningen ha direkt åtkomst till register med uppgifter om DNA-analyser i brottmål. Polismyndigheternas och Åklagarmyndighetens åtkomst är dock begränsad till uppgifter om huruvida någon förekommer i ett sådant register.

Enligt 28 kap. 14 § rättegångsbalken samt förordningen (1992:824) om fingeravtryck m.m. ska fingeravtryck och fotografi alltid tas av den som häktats. I vissa uppräknade fall ska fingeravtryck och fotografi också tas av den som är anhållen. Fingeravtrycket och fotografiet ska enligt 7 § förordningen skyndsamt sändas till Rikspolisstyrelsen tillsammans med en beskrivning av personen.

Rikspolisstyrelsen för ett fingeravtrycksregister och ett signalements- och känneteckensregister med stöd av tillstånd från Datainspektionen från år 1976. Enligt övergångsbestämmelserna till polisdatalagen ska datalagen (1973:289) tillämpas på personregister som den 24 oktober 1998 fördes med stöd av Datainspektionens tillstånd. Övergångsbestämmelserna har förlängts flera gånger och gäller för närvarande till utgången av december 2009. I propositionen Övergångsbestämmelserna till polisdatalagen (prop. 2009/10:23) har föreslagits ytterligare förlängning till utgången av juni 2012. Fingeravtrycksregistret och signalements- och känneteckensregistret förs således med stöd av övergångsbestämmelserna till polisdatalagen.

Eftersom registren fortfarande förs med stöd av lagens övergångsbestämmelser tillämpas inte bestämmelserna i 29–31 §§ polisdatalagen om fingeravtrycks- och signalementsregister på de aktuella registren. Bestämmelserna behandlar bl.a. sådana registers ändamål och innehåll. Uppgifter får behandlas för att underlätta identifiering av personer i samband med brott. De får också användas för identifiering av okända personer i andra fall. De får vidare behandlas i förundersökningar och särskilda undersökningar. Bestämmelserna i polisdatalagen om ändamål och innehåll överensstämmer i stort med den hittillsvarande användningen av ifrågavarande register.

Polisdatalagen innehåller även en bestämmelse om gallring. Där föreskrivs att uppgifter i fingeravtrycks- och signalementsregister om en misstänkt person ska gallras när förundersökning eller åtal mot personen läggs ned eller när åtal mot personen ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den registrerade ska behandlas med stöd av polisdatalagens regler om behandling av uppgifter om kvarstående misstankar. Om den registrerade döms, ska uppgifterna gallras senast då uppgifterna gallras ur belastningsregistret. Datainspektionen har genom beslut den 1 december 2005, 20 juni 2006 och 10 oktober 2008 meddelat gallringsbestämmelser för fingeravtrycksregistret respektive signalements- och känneteckensregistret. Bestämmelserna för fingeravtrycksregistret överensstämmer i sak med polisdatalagens bestämmelse om gallring medan bestämmelserna för signalements- och känneteckensregistret är något annorlunda utformade. I sistnämnda bestämmelser varierar gallringstiden beroende på det misstänkta brottets svårhetsgrad.

SÄPO-registret

Enligt 32 § polisdatalagen ska Säkerhetspolisen föra ett SÄPO-register. Registret beskrivs nedan.

Det allmänna spaningsregistret

Det allmänna spaningsregistret förs av Rikspolisstyrelsen med tillstånd av Datainspektionen enligt beslut den 18 maj 1977 och med stöd av övergångsbestämmelserna till polisdatalagen. Registret ska enligt sin ändamålsbeskrivning lagra och systematisera uppgifter med anknytning till misstänkt eller konstaterad brottslighet för att användas i polisens spanande och brottsutredande verksamhet. Både Rikspolisstyrelsen och polismyndigheterna kan behandla uppgifter i registret.

Det allmänna spaningsregistret syftar till att bygga upp kunskaper om och kring personer som misstänks för brott. Registret utgår från misstänkta gärningsmän. En person registreras i det allmänna spaningsregistret om det finns misstanke om att han eller hon begått ett brott. Uppgifterna i registret kommer från brottsanmälningar och förundersökningsprotokoll, men registrering kan också ske på grund av trovärdiga tips från t.ex. personal inom socialförvaltningen.

Det är ett krav för registrering att det alltid finns en grundhandling varifrån den registrerade uppgiften är hämtad. En referens till denna grundhandling ska antecknas i registret tillsammans med uppgiften. På grundhandlingen antecknas vem som fattat beslut om registreringen och vem som rent faktiskt utfört registreringen.

Olika uppgifter om den misstänkte får registreras, bl.a. namn och personnummer, alternativa förnamn och efternamn, adresser där personen brukar vistas, speciella fysiska kännetecken, intressenter (alla som bidrar med uppgifter om personen) och senaste händelse inom kriminalvården. Registret innehåller också andra uppgifter kopplade till personen. Det registreras vilka brottstyper som personen ägnar sig åt (hans modus operandi), händelseanteckningar som rör tidigare brottsmisstankar, anknytning till andra personer och spaningsinformation rörande brottsmisstankar.

En speciell typ av noteringar i registret är de så kallade A-markeringarna och Y-markeringarna för misstänkta. En A-markering för en misstänkt person betyder att personen är synnerligen allvarligt brottsbelastad. A-markeringar sätts enbart av Rikskriminalpolisen. En Y-markering talar om att den misstänkte bedöms vara yrkeskriminell. Denna markering sätts av polismyndigheterna.

Vid sökningar i registret kan man variera mellan ett eller flera sökbegrepp. Dessa sökbegrepp kan dock inte varieras helt fritt utan det finns begränsningar i sökmöjligheterna. Man kan t.ex. söka på ålder och något speciellt fysiskt kännetecken och på det viset få fram alla personer som svarar mot de sökbegreppen. Registret innehåller också uppgifter om personer med anknytning till den misstänkte. Dessa ”anknytningspersoner” behöver inte vara misstänkta för brott för att registrering ska få ske. Deras namn är dock inte sökbara i registret, om de inte själva är misstänkta för brott.

Det allmänna spaningsregistret innehåller omkring 100 000 sökbara personer. Antalet personer har sedan lång tid legat konstant på den nivån.

Uppgifter i registret gallras efter 18 månader, tre år eller fem år beroende på brottets svårighetsgrad. Uppgifter får bevaras längre om en ny

uppgift om personen antecknas före gallringstidens utgång. A- eller Y-markering utgör hinder mot gallring. Gallringen sker automatiskt med hjälp av ett särskilt gallringsprogram.

All tillgång till uppgifter i registret för enskilda befattningshavare styrs av personligt tilldelad behörighet. Polismyndigheterna beslutar om vilka personer som ska ha sådan behörighet. Ett ytterligare begränsat antal personer har behörighet att föra in uppgifter i registret. Enligt 14 § polisdataförordningen får polismyndigheter och Ekobrottsmyndigheter ha direktåtkomst till det allmänna spaningsregistret. Uppgifter ur registret får enligt 15 § lämnas till Tullverket, Kustbevakningen och Skatteverket, om uppgifterna kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

Det centrala brottsspaningsregistret

Det centrala brottsspaningsregistret förs av Rikspolisstyrelsen med tillstånd från Datainspektionen och med stöd av övergångsbestämmelserna till polisdatalagen. För en närmare redogörelse för tillkomsten av registret, se regeringsbeslut den 21 februari 2008 i ärende Ju2005/8197/PO.

Ändamålet med det centrala brottsspaningsregistret är att skapa ett särskilt brottsregister över anmälda allvarligare brott som kan utnyttjas i brottsspanings- och brottsutredningsverksamhet samt i annan därmed jämförlig polisiär verksamhet. Även mindre allvarliga brott får dock registreras.

Det centrala brottsspaningsregistret innehåller uppgifter om anmälda brott, tillvägagångssätt, signalement beträffande personer som setts på brottsplatsen, motsvarande uppgifter om fordon och spår från brottsplatsen m.m. Registret skiljer sig från det allmänna spaningsregistret genom att centrala brottsspaningsregistret utgår från brott och inte från misstänkta gärningsmän. Det kan sägas vara ett register över modus operandi. Uppgifter till registret kommer från systemet rationell anmälningsrutin (RAR, se nedan). Det är framför allt allvarliga brott som registreras. Rikspolisstyrelsen har föreskrivit vilka brott som ska antecknas i centrala brottsspaningsregistret. Personuppgifterna i registret utgörs av noteringar om misstänkta gärningsmän.

Registret innehåller noteringar om ungefär 129 000 brott. Det används inom polisen för att t.ex. söka liknande tillvägagångssätt (modus operandi) vid andra brott eller brott som har förövats av samma person. Ibland kan man finna att personer med samma signalement har synts vid flera brott av samma typ.

All tillgång till uppgifter ur det centrala brottsspaningsregistret styrs av personligt tilldelad behörighet. Polismyndigheterna beslutar själva om vilka som ska ha denna behörighet. Ett mindre antal personer har behörighet att föra in uppgifter i registret.

Beslags- och analysregister

Beslags- och analysregistren förs av Rikspolisstyrelsen och polismyndigheterna med tillstånd meddelat av Datainspektionen den 6 november

1987 och med stöd av övergångsbestämmelserna till polisdatalagen. Enligt Datainspektionen får delregistren anses förda för respektive myndighets verksamhet, vilket innebär att myndigheterna är personuppgiftsansvariga för sina egna register.

Ändamålet med registren är enligt tillståndet

– dels underlag för undersökning av modus operandi och profiler av strategisk och taktisk betydelse för den nationella och internationella narkotikabekämpningen,

– dels rapportering av analysresultat avseende beslagtagen narkotika samt framställning av statistik.

Syftet är att analysresultat snabbt ska kunna bli tillgängliga för Rikspolisstyrelsen och respektive narkotikarotel via bildskärm. Analysdelen av registren innehåller uppgift om det misstänkta preparatet och motsvarande beslagsnummer. Vidare anges namn och personnummer på den person hos vilken beslaget gjorts. I registret antecknas också uppgifter om bl.a. modus operandi, transportmedel, eventuell beslagtagen valuta och eventuella vapen. Dessutom ska den beslagtagna narkotikan beskrivas samt var och när den anträffades.

Finanspolisens analys- och spaningsregister

Finanspolisens analys- och spaningsregister inrättades år 1994 med stöd av ett tillstånd från regeringen den 16 december 1993. Datainspektionen meddelade den 27 januari 1994 föreskrifter för registret. Registret omfattas inte av övergångsbestämmelserna i polisdatalagen eftersom det inte fördes med tillstånd från Datainspektionen utan med stöd av ett tillstånd från regeringen. Enbart bestämmelserna i personuppgiftslagen och polisdatalagen är därmed tillämpliga på registret.

Registret består av två delregister, Finanspolisens analys- och förspaningsregister samt Finanspolisens diarium. Finanspolisens analys- och förspaningsregister utgör ett hjälpmedel i Rikspolisstyrelsens spanings- och analysverksamhet i ärenden hos Finanspolisen som avser sådana förfaranden som anges i lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). En del av uppgifterna i registret har underrättelsekaraktär. Registret används även för framställning av statistik. Ändamålet med Finanspolisens diarium är att utgöra ett diarium enligt 5 kap. offentlighets- och sekretesslagen (2009:400).

Registret får innehålla uppgifter som rapporteras till Rikspolisstyrelsen enligt penningtvättlagens bestämmelser eller från andra polismyndigheter eller motsvarande utländska samarbetspartners eller som framkommit i Finanspolisens spanings- och analysverksamhet, under förutsättning att det finns skäl att anta att transaktionen avser medel som härrör från ett brottsligt förvärv av allvarligare slag. Registret får även innehålla uppgifter som rapporteras till Rikspolisstyrelsen från Tullverket eller verkets utländska samarbetspartners i deras brottsbekämpande verksamhet, under förutsättning att det finns skäl att anta att transaktionen avser medel som härrör från ett brottsligt förvärv av allvarligare slag. Vidare får registret innehålla uppgifter som härrör från andra källor än vad som sägs ovan, om de bedöms vara av betydelse för utredningen av det aktuella ärendet.

Barnpornografiutredningen föreslog i sitt betänkande Barnpornografifrågan (SOU 1997:29) att en internationellt tillgänglig databank med barnpornografiska framställningar skulle inrättas i Sverige med Rikspolisstyrelsen som huvudansvarig.

Efter en ansökan från Rikspolisstyrelsen beslutade regeringen den 18 september 1997 att det hos Rikspolisstyrelsen skulle inrättas och föras ett personregister med namnet Digitalt referensbibliotek över barnpornografiska framställningar. Ändamålet med registret är enligt beslutet att utföra bildanalys i brottsutredningar samt att bistå utländska brottsutredande myndigheter med uppgifter om bildanalys i brottsutredningar. Innehållet i registret ska bestå av kopior av barnpornografiska framställningar som tagits i beslag. Registret får också innehålla barnpornografiska framställningar som överlämnats av en utländsk brottsutredande myndighet. Registret får även innehålla uppgifter om var framställningen tagits i beslag.

Registret omfattas inte av övergångsbestämmelserna i polisdatalagen eftersom det inte förs med tillstånd av Datainspektionen utan med stöd av ett regeringsbeslut. Enbart bestämmelserna i personuppgiftslagen och polisdatalagen är därför tillämpliga på behandlingen av personuppgifter i registret. Till följd av detta har en särskild undersökning enligt polisdatalagens bestämmelser inletts som omfattar den behandling av personuppgifter som är nödvändig i arbetet med att förebygga och beivra brott relaterade till barnpornografi.

Personefterlysnings- och U-boksregistret

Personefterlysnings- och U-boksregistret utgör det s.k. EPU-systemet (efterlysta personer och U-boken). Systemet förs med tillstånd av Datainspektionen den 11 oktober 1977 och med stöd av övergångsbestämmelserna till polisdatalagen. Registret består av två delregister; EP-delen och U-boksdelen.

Ändamålet med registret är enligt tillståndet att

– dels i enlighet med efterlysningskungörelsen (1969:293) föra register över efterlysningar och utge förteckningar över gällande efterlysningar och över efterlysningar som har återkallats,

– dels i enlighet med 5 § andra stycket lagen (1965:94) om polisregister m.m. sammanställa och sända ut uppgifter från polisregister om avlägsnanden ur riket och beslut som har samband därmed,

– dels använda de registrerade uppgifterna vid utredningar i passärenden enligt passkungörelsen (1941:836) och vid passkontroll enligt utlänningskungörelsen (1969:136) samt vid annan därmed jämförlig polisiär verksamhet.

Av 2 § efterlysningskungörelsen framgår att efterlysning verkställs genom att uppgifter införs i ett register över efterlysta personer som förs med ADB. Rikspolisstyrelsen, polismyndighet, åklagarmyndighet eller Kriminalvården beslutar om efterlysning. Annan myndighet kan göra framställning hos polisen om efterlysning. Uppgifter om personefterlysningar införs i EP-delen av registret.

För framställning av U-boken antecknar Rikspolisstyrelsen i ett centralt register uppgifter om den som utvisats ur Sverige på grund av brott samt uppgifter om den som avvisats eller utvisats enligt beslut av Migrationsverket, en migrationsdomstol, Migrationsöverdomstolen eller regeringen i de fall där beslutet är förenat med ett återreseförbud.

Personefterlysningsregistret innehåller känsliga personuppgifter i personuppgiftslagens mening, såvitt avser anledningen till efterlysningen. En sådan anledning till efterlysning kan t.ex. vara att personen avvikit från ett behandlingshem för vård av missbrukare.

Godsregister

Godsregistret förs med tillstånd meddelat av Datainspektionen den 23 juni 1977 och med stöd av övergångsbestämmelserna till polisdatalagen. Ändamålet med registret är enligt tillståndet följande. I registret antecknas gods som stulits, förkommit eller omhändertagits, t.ex. såsom hittegods, eller som har beslagtagits vid husrannsakan. Registret används i polisens spanings- och utredningsverksamhet för att identifiera sådant gods. Registret används vidare för att kontrollera gods som pantsatts hos pantlånerörelser och liknande inrättningar. Det kan även – efter förfrågan från en enskild person till vederbörande polismyndighet – användas för kontroll av gods som utbjudits till enskild person för försäljning. Registret utgör också underlag för viss statistik avseende arten och värdet av gods m.m. Godsregistret håller på att avvecklas.

Efterlysningssystem för fordon m.m.

Efterlysningssystemet för fordon m.m. förs med tillstånd meddelat av Datainspektionen den 23 juni 1986 och med stöd av övergångsbestämmelserna till polisdatalagen.

Ändamålet med registret är enligt tillståndet att utgöra underlag och hjälpmedel för den polisiära spaningsverksamheten samt att sprida upplysning inom polisen och till bl.a. vissa andra myndigheter om fordon som efterlysts.

De personer som får registreras är ägare till fordon som ska efterlysas (omkring 40 000 per år), person som anträffar ett efterlyst fordon (omkring 10 000 per år) samt person som efterspanas och som kan misstänkas färdas med ett visst fordon som ägs av annan (omkring 400 per år). De uppgifter som får anges är bl.a. uppgifter om fordonet, ägarens personnummer eller organisationsnummer, ägarens namn, anledning till efterlysningen, handläggande polismyndighet och diarienummer samt var och när fordonet anträffades. Av Datainspektionens beslut framgår att fritext bara får innehålla uppgifter av den art som exemplifieras i ansökningen. I ansökningen sägs att fritext inte ska innehålla uppgift om brott eller brottsmisstanke.

Passregistret

Enligt 23 § passförordningen (1979:664) ska Rikspolisstyrelsen föra dels ett centralt passregister, dels ett centralt register över personer som, på

grund av att de genomgår viss psykiatrisk vård, behöver passtillstånd enligt 20 § passlagen (1978:302).

Registren förs av Rikspolisstyrelsen och polismyndigheterna. Sedan den 1 oktober 2001 förs registren med stöd av personuppgiftslagen. Ändamålet med registren är att tillhandahålla uppgifter som behövs för att utfärda pass, för att kontrollera vilka personer som innehar pass, för att hindra att någon innehar mer än ett pass, för att kontrollera om passtillstånd fordras, för identifieringskontroll i polisens verksamhet samt för kontroll och avstämning av passuppgifter, passböcker och avgifter.

Passregistret får innehålla uppgift om bl.a. passinnehavarens identitet, passnummer, passets giltighetstid och kod för särskilt passhinder.

Registret för identifiering av försvunna personer

Registret för identifiering av försvunna personer förs med tillstånd meddelat av Datainspektionen den 16 juni 1988 och med stöd av övergångsbestämmelserna till polisdatalagen. Ändamålet med registret är enligt tillståndet att underlätta framtagning av detaljerade signalementsuppgifter om personer som varit försvunna en längre tid och därvid underlätta identifieringen av okända och avlidna personer.

I registret förs uppgifter om personer som anmälts försvunna och som registrerats i personefterlysnings- och U-boksregistret (se ovan) samt inte återfunnits efter sextio dagar.

Disaster Victim Identification

Registret Disaster Victim Identification (DVI-registret) förs med tillstånd av meddelat av Datainspektionen den 15 oktober 1998 och med stöd av övergångsbestämmelserna till polisdatalagen.

DVI-registret består av blanketter som tagits fram inom Interpol för registrering av uppgifter om försvunna personer och om oidentifierade människokroppar. Registret innehåller mycket detaljerade uppgifter om de registrerade och många av uppgifterna i registret utgör känsliga personuppgifter i personuppgiftslagens mening. Detta gäller t.ex. uppgifter om religiös övertygelse, om smittsamma infektioner, om användning av läkemedel och annan information från läkarjournaler.

Register med anknytning till det statliga person- och adressregistret

Polisens adressdatabas, polisens fastighetsfråga, polisens historikdatabas och polisens folkbokföringsdatabas är register av administrativ karaktär. De fyra registren har alla samband med det statliga person- och adressregistret (SPAR) som förs med stöd av lagen (1998:527) om det statliga personadressregistret.

Adressdatabasen förs med tillstånd av Datainspektionen meddelade den 3 mars och 16 april 1992. Ändamålet med registret är att ge polisen upplysning om vilka personer som är folkbokförda på en viss adress för att därmed utgöra ett stöd i sådan hjälpande verksamhet som avses i 2 § 4 polislagen. Dessutom ska registret utgöra ett stöd i polisens spaning och utredning i fråga om brott som hör under allmänt åtal. I ansökan om

tillstånd anges att registret endast ska innehålla uppgifter om ”personer folkbokförda i Sverige med undantag för de som sekretessmärkt sina adresser i folkbokföringen”. De uppgifter som registreras är personnummer, gatuadress och ”markering om personens gatuadress är aktuell eller ej”. Även vissa personer anknutna till den folkbokförde registreras, bl.a. maka eller make och vårdnadshavare. Adressdatabasen innehåller också uppgifter om personer som har varit folkbokförda och som är avregistrerade från folkbokföringen. Registret bygger på information från SPAR.

Polisens fastighetsfråga förs med tillstånd av Datainspektionen meddelade den 24 september 1993 och 15 september 1997. Ändamålet med registret är enligt tillståndet att ge polisen upplysning om fastighet (fastighetsbeteckning) hörande till viss person. Registret får bara innehålla uppgifter om personer som är folkbokförda i Sverige. Inga andra uppgifter än personnummer och fastighetsbeteckning förs in i registret.

Polisens historikdatabas förs med tillstånd av Datainspektionen meddelade den 24 september 1993, 21 januari 1997 och 15 december 1997. Ändamålet med registret är att ge polisen upplysning om uppgifter som gallrats ur SPAR avseende personer under 90 år. Endast personer som är folkbokförda i Sverige registreras.

Polisens folkbokföringsdatabas förs med stöd av Datainspektionens tillstånd den 16 december 1997. Innehållet i registret består av folkbokföringsuppgifter som ingår i Riksskatteverkets Aviseringsregister men som inte får ingå i SPAR.

Säkerhetspolisens system

Allmänt

I Säkerhetspolisens verksamhet används flera olika databaser som innehåller personuppgifter. Det rör sig om SÄPO-registret, centralregistret, systemet för hemlig teleavlyssning och hemlig teleövervakning samt analysdatabaser.

Utöver det i polisdatalagen särskilt reglerade SÄPO-registret styrs behandlingen av personuppgifter i Säkerhetspolisens verksamhet av bestämmelserna i personuppgiftslagen, polisdatalagens allmänna del och arbetsordningen för Säkerhetspolisen.

SÄPO-registret

SÄPO-registret är ett register som är avsett för den särskilda polisverksamhet som Säkerhetspolisen bedriver. Bestämmelserna om SÄPO-registret finns i 32–35 §§ polisdatalagen. Polisdatalagen föreskriver att Säkerhetspolisen ska föra ett register (SÄPO-registret) som har till ändamål att

– underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
– underlätta spaning i syfte att bekämpa terrorism och
– utgöra underlag för registerkontroll enligt säkerhetsskyddslagen (1996:627).

SÄPO-registret får innehålla uppgifter som kan hänföras till en enskild person endast
– om den uppgifterna gäller kan misstänkas för att ha utövat eller komma att utöva brottslig verksamhet som innefattar hot mot rikets säkerhet eller terrorism,
– om personen har undergått registerkontroll enligt säkerhetsskyddslagen eller
– om det med hänsyn till registrets ändamål annars finns särskilda skäl till det.

Registrerade uppgifter ska gallras senast tio år efter det att en sådan uppgift om personen som kan föranleda registrering senast infördes. Om det finns särskilda skäl får dock uppgifterna stå kvar under längre tid.

Enligt 13 § polisdataförordningen är direktåtkomst till uppgifter i SÄPO-registret eller till uppgifter som i annat fall behandlas automatiserat hos Säkerhetspolisen förbehållen de personer som på grund av sina arbetsuppgifter behöver informationen.

SÄPO-registret är avsett att vara ingången till Säkerhetspolisens hantering av personuppgifter (prop. 1997/98:97 s. 154). Registret innehåller endast identifieringsuppgifter, uppgifter om grunden för registrering och hänvisning till de ärenden där uppgifter om den registrerade behandlas. Registret fyller inte någon operativ funktion i Säkerhetspolisens verksamhet. All behandling av personuppgifter av betydelse för verksamheten sker i andra system. Registret förs enbart för att uppfylla kravet i 32 § polisdatalagen att Säkerhetspolisen ska föra ett sådant register.

Säkerhetspolisens centralregister

Säkerhetspolisens centralregister är den databas som huvudsakligen används i Säkerhetspolisens verksamhet. Centralregistret kan sägas utgöra en ingång till den samlade personuppgiftshanteringen hos Säkerhetspolisen.

Det övergripande ändamålet med centralregistret är att det ska utgöra ett spaningsregister i Säkerhetspolisens verksamhet för att förebygga och avslöja brott mot rikets säkerhet och för att bekämpa terrorism. Vidare används uppgifter ur databasen som underlag för registerkontroll enligt säkerhetsskyddslagen.

Databasen innehåller uppgifter om personer mot vilka det föreligger misstankar om brottslig verksamhet, som inte behöver vara preciserade till vissa konkreta brott. I databasen behandlas även uppgifter om personer som har samband med någon som antecknats på grund av en misstanke. Vidare behandlas uppgifter om personer som kan bli utsatta för hot av olika slag eller som i känsliga verksamheter kan bli föremål för närmanden från utländska underrättelsetjänster.

Personuppgifter noteras i centralregistret i den utsträckning som uppgifterna behövs för databasens ändamål.

Känsliga personuppgifter antecknas som kompletterande uppgifter, om en viss persons uppträdande ger anledning anta anta att personen kan misstänkas för sådana brott som Säkerhetspolisen ska ingripa mot. Om det är oundgängligen nödvändigt att en känslig personuppgift noteras för att viss information i registret ska bli begriplig får notering ske. Det sist-

nämnda innebär t.ex. att uppgifter om en misstänkts eller hotad persons politiska tillhörighet kan komma att antecknas.

Uppgifterna i centralregistret är tillgängliga för Säkerhetspolisens operativa personal enligt särskilda behörighetsregler.

Systemet för hemlig teleavlyssning och hemlig teleövervakning

Systemet för hemlig teleavlyssning och hemlig teleövervakning utgör ett bearbetnings- och analysverktyg vid behandling av uppgifter som inhämtats genom hemlig teleavlyssning eller hemlig teleövervakning. Systemet innehåller personuppgifter i den utsträckning sådana uppgifter behövs för behandlingens ändamål.

De personuppgifter som antecknas i systemet utgörs av uppgifter om abonnenter och teleadresser som är kopplade till ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning. Vidare antecknas uppgifter om kontakter och teleadresser som uppmärksammas med anledning av en pågående teleavlyssning eller teleövervakning. Dessutom noteras innehållet i telefonsamtal och andra telemeddelanden samt utredningsanteckningar.

Uppgifterna i systemet utgörs till en början av obearbetade underrättelser som i en bestämd utredning inhämtats genom något av de nyss nämnda tvångsmedlen. De inhämtade uppgifterna bearbetas och analyseras. Efter bearbetning och analys tas de uppgifter bort som inte är relevanta för utredningen. Övriga uppgifter tillförs centralregistret. Uppgifterna i systemet är tillgängliga för de befattningshavare som har behörighet att arbeta med det aktuella ärendet.

Analysdatabaser

Analysdatabaserna innehåller liksom systemet för hemlig teleavlyssning och hemlig teleövervakning underrättelser som är avsedda att bearbetas. Underrättelserna i analysdatabaserna inhämtas genom uppgifter från källor, genom spaning samt genom tvångsmedel som t.ex. hemlig teleavlyssning och hemlig teleövervakning. Personuppgifter antecknas om uppgifterna behövs för behandlingens ändamål.

Bearbetad och bedömd information förs över till centralregistret, medan uppgifter som inte behövs gallras under utredningens gång.

Uppgifter i en analysdatabas är tillgängliga endast för de befattningshavare som är behöriga att arbeta med det aktuella ärendet. En analysdatabas får inrättas efter beslut från chefen för dokumentationsenheten hos Säkerhetspolisen.

Lokala system med nationell spridning

Allmänt

Polismyndigheterna har inrättat flera olika system för automatiserad behandling av uppgifter. Det gäller bl.a. s.k. tillhållsregister samt system för intern samordning av pågående utredningar. Att ett system är lokalt innebär att det i princip bara är den egna polismyndigheten som har till-

gång till uppgifter ur systemet. Här redovisas fyra lokala system som har nationell spridning, nämligen rationell anmälningsrutin, datoriserad utredningsrutin – tvångsmedel, kommunikationscentralernas system och förundersökningsregister.

Rationell anmälningsrutin

Rationell anmälningsrutin (RAR) förs av polismyndigheterna, med tillstånd meddelade av Datainspektionen den 17 september 1993 och 17 december 1997 och med stöd av övergångsbestämmelserna till polisdatalagen.

Rikspolisstyrelsen har den 28 januari 1998 av Datainspektionen meddelats tillstånd att föra RAR, för att stödja Rikskriminalens brottsutredande verksamhet. Ekobrottsmyndigheten har den 18 februari 1998 beviljats tillstånd att föra RAR i sin polisiära verksamhet. Registren förs med stöd av tillstånden och övergångsbestämmelserna till polisdatalagen.

Ändamålen med registren är

– att tillhandahålla uppgifter om brottsanmälningar som behövs i den registeransvariges brottsutredande verksamhet och som behövs för att Rikspolisstyrelsen skall kunna fullgöra sin stödjande, samordnande och förstärkande verksamhet,
– service åt allmänheten och att i enlighet med lag eller förordning lämna uppgifter till annan myndighet, samt
– att tillhandahålla uppgifter för polismyndighetens ärenden, lämna underlag för samordning, bevakning, planering och uppföljning av verksamheten, utgöra underlag för registrering av uppgifter i misstankeregistret och produktion av statistik samt tillika utgöra myndighetens kriminaldiarium.

RAR innehåller uppgifter från polisens brottsanmälningar. En brottsanmälan förs in i RAR direkt, med undantag för brottsanmälningar som görs av allmänheten via Internet. Nära nog alla brottsbalksbrott registreras i RAR. Dessutom registreras brott mot speciallagstiftning. Trafikbrott registreras i T–RAR.

Samtliga uppgifter i brottsanmälningarna registreras i RAR. Förutom uppgifter om själva brottet finns personuppgifter avseende målsägande, anmälare, skäligen misstänkt gärningsman, vittne samt försvunna och avlidna personer.

Datoriserad utredningsrutin

Systemet datoriserad utredningsrutin – tvångsmedel (DurTvå) är ett lokalt datasystem med nationell spridning. Det syftar till att effektivisera polisens och åklagarnas arbete med förundersökningar i brottmål. Systemet regleras av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen.

I DurTvå upprättas förundersökningsprotokoll elektroniskt. För att en brottsanmälan ska registreras i DurTvå krävs dels ett beslut om att inleda förundersökning, dels ett beslut om att ärendet ska föras över från RAR. Eventuella tilläggsanmälningar förs däremot automatiskt över till DurTvå.

Genom DurTvå har användaren tillgång till tvångsmedelstjänsten, som numera utgör polismyndigheternas beslagsliggare.

Det finns ett behörighetssystem för sökning i DurTvå. Behörigheten att få del av uppgifter är uppdelad i tre nivåer.

Kommunikationscentralernas system

För att effektivisera och samordna bl.a. alarmeringsåtgärder och viss tillfällig spaningsverksamhet ska varje län ha en kommunikationscentral. Uppgifterna för kommunikationscentralerna är att ta emot och vidarebefordra inkommande larm och andra meddelanden samt att inledningsvis vidta och samordna polisåtgärder med anledning av dessa.

För denna verksamhet finns det ett särskilt systemstöd för kommunikationscentralerna, det s.k. KC-systemet. Behandlingen av personuppgifter i systemet sker med stöd av bestämmelserna i personuppgiftslagen och i de allmänna bestämmelserna i polisdatalagen. Det finns motsvarigheter till KC-systemet i flera andra europeiska länder och även i USA.

Huvudsyftet med behandlingen är att dokumentera, bevaka och följa upp händelser och iakttagelser som rapporteras till kommunikationscentralerna. Ett annat syfte är att på ett tidigt stadium erhålla signaler om pågående och återkommande brottslig verksamhet, exempelvis om familjevåld och mc-brottslighet. Vidare har behandlingen till ändamål att ge underlag för planering av polisens resurser och för uppföljning av verksamheten.

I KC-systemet registreras uppgifter om brotts- eller händelseplatser med besked om tid, plats, händelsetyp, brottskod och övrig information som kan vara till hjälp vid en kommande polisutredning. Systemet innehåller också personuppgifter. Anmälare, målsägande, vittne, misstänkta, utpekade och försvunna personer samt personer som på olika sätt kontaktar polisen i ärenden registreras i KC-systemet. I Stockholm noteras 1 000–1 200 ärenden per dygn i KC-systemet.

Rikspolisstyrelsen har i enlighet med 2 § polisdataförordningen anmält KC-systemet till Datainspektionen för förhandskontroll. Inspektionen har i beslut den 21 december 1999 framfört synpunkter på rutinerna för gallring och för information till de registrerade.

Enligt anmälan ska de registrerade uppgifterna i händelserapporterna vara tillgängliga i KC-systemet under 13 månader. Datainspektionen har erinrat om att personuppgifter som behandlas automatiserat enligt huvudregeln i 13 § polisdatalagen ska gallras när uppgifterna inte längre behövs för sitt ändamål.

I fråga om information till registrerade sägs i anmälan att information om uppgiftsbehandling inte ska lämnas annat än till vissa särskilt angivna kategorier av personer. Rikspolisstyrelsen har därvid hänvisat till bestämmelsen i 24 § tredje stycket personuppgiftslagen, som föreskriver att information får underlåtas om lämnandet skulle visa sig vara omöjligt eller innebära en oproportionerligt stor arbetsinsats. Datainspektionen har anfört att denna undantagsbestämmelse inte kan anses vara generellt tillämplig i fråga om samtliga angivna kategorier av registrerade.

Datainspektionen meddelade den 5 maj 1976 beslut om tillstånd att föra förundersökningsregister. Ändamålet med registren är att utgöra hjälpmedel för att lagra, systematisera och återvinna uppgifter i förundersökningar med komplicerat eller omfattande utredningsmaterial.

Förundersökningsregister får enligt Datainspektionens beslut endast innehålla uppgifter av den art som framgår av ansökningen. Förutom administrativa uppgifter får registreras uppgifter om namn på uppgiftslämnare, uppgifter om en person som kan sättas i samband med något brott, beskrivning av fordon och personer, uppgifter om brottsplats, uppgifter ur förhör samt uppgifter om adresser till kända ”tillhåll” och ”kvartar”.

Intranät

Polisens intranät används i första hand för att sprida verksamhetsrelaterad information inom polismyndigheterna.

IntraPolis

IntraPolis är ett nationellt nätverk. Olika polismyndigheter har utvecklat intranät för respektive myndighet och dessa intranät utgör delar av IntraPolis. Genom polismyndigheternas intranät förmedlas både öppen och skyddad information. På intranäten finns även information som omfattas av sekretess. Den öppna informationen är tillgänglig för alla inom polisen medan det erfordras särskild behörighet inom respektive polismyndighet för att få tillgång till den skyddade informationen.

Ett exempel på skyddad information är s.k. KUT-Info.

KUT-Info

I fråga om behandlingen av personuppgifter i KUT-Info gäller bestämmelserna i personuppgiftslagen och polisdatalagen. Konsekvenserna av dessa regelverk för behandling av personuppgifter på intranät belyses i ett beslut från Datainspektionen den 28 januari 2000. Beslutet föranleddes av att Polismyndigheten i Stockholms län enligt 2 § polisdataförordningen hade anmält att myndigheten i systemet KUT-Info avsåg att behandla personuppgifter som gav upplysning om att personer var dömda eller misstänkta för brott.

I förhandsanmälan till Datainspektionen anförde polismyndigheten beträffande en planerad behandling av personuppgifter i KUT-Info bl.a. följande.

Inom Stockholms län ska distribueras kriminalunderrättelseinformation, förkortat KUT-Info, från länskriminalens underrättelserotel ett par gånger i veckan. Informationen ska bestå av uppgifter om efterlysta personer, om oidentifierade gärningsmän, om framställningar från olika utredningsmän om hjälp, om permissioner, om brott av polisiärt intresse som uppgifter angående t.ex. dolda vapen och om tillvägagångssätt vid brott m.m. Uppgifterna ska spridas genom IntraPolis till omkring 400 an-

vändare, som i sin tur ska skicka uppgifterna vidare till ytterligare ett stort antal poliser och andra anställda inom myndigheten. KUT-Info ska skickas främst till anställda hos Polismyndigheten i Stockholms län men även till behöriga tjänstemän inom andra polismyndigheter i Sverige. Syftet med den planerade nya behandlingen är att utnyttja den moderna tekniken och använda IntraPolis för snabb publicering av kriminalunderrättelseinformation samt att snabbt sprida väsentlig information som polisanställda har behov av i sin tjänst.

Uppgifterna beträffande efterlysta personer ska omfatta namn, personnummer, foto, adressuppgifter samt fordon. Dessutom kommer uppgifter om vilka brott personen är efterlyst för samt uppgifter om farlighet att anges. Polisen avser även att sprida fotografier på oidentifierade personer som är misstänkta för brott. Även fotografier och uppgifter om värdefullt tillgripet gods ska spridas. Uppgifter beträffande personer som är dömda för grova brott samt tidpunkterna för dessa personers permissioner och frigivning från avtjänande av påföljder kommer att nämnas i KUT-Info.

I beslutet den 28 januari 2000 rörande behandling av personuppgifter i KUT-Info framhöll Datainspektionen att frågan om i vilken utsträckning den aktuella informationsförmedlingen ska kunna förekomma och vilka uppgifter som ska kunna presenteras borde bli föremål för central reglering, åtminstone genom sådana föreskrifter som förutsätts i 17 § polisdataförordningen. Vidare uttalade Datainspektionen att enligt dess mening är behandling och registrering av personuppgifter i kriminalunderrättelseverksamhet uttömmande reglerad i polisdatalagen. Det är inte förenligt med polisdatalagen att i ett system som KUT-Info behandla personuppgifter som faller under begreppet kriminalunderrättelseverksamhet.

Med anledning av Datainspektionens beslut anpassade Polismyndigheten i Stockholms län behandlingen och driftsatte under våren 2000 ett KUT-infosystem. Även andra länspolismyndigheter har i likhet med polismyndigheten i Stockholms län infört system för KUT-info.

DAR

Rikspolisstyrelsen har huvudansvaret för polisens internationella kontakter. Vid Rikskriminalpolisen finns en enhet som fungerar som nationell kontaktpunkt och sambandskontor för det internationella polissamarbetet. Detta genererar en mycket stor mängd ärenden årligen, som hanteras i ett dokument- och ärendehanteringssystem benämnt DAR. Systemet förs med stöd av polisdatalagens allmänna bestämmelser och personuppgiftslagen.

DAR används för all diarieföring, dokument- och ärendehantering vid Rikskriminalpolisens enhet för internationellt polissamarbete, med undantag för underrättelseinformation. DAR är ett elektroniskt system som hanterar all information i sin helhet. Dokument, textfiler, bilder, fax och skannade bilagor lagras i systemet. DAR innefattar förutom ärendehantering även en funktion för elektronisk gallring, avställning och arkivering.

En uppdelning av uppgifter på belastningsuppgifter och misstankeuppgifter

I Europarådets rekommendation No. R (87) 15 om användning av personuppgifter inom polissektorn anges att olika kategorier av uppgifter så långt det är möjligt ska hållas åtskilda efter graden av riktighet och tillförlitlighet. I propositionen Riktlinjer för registreringen av påföljder m.m. (prop. 1994/95:144) uttalade regeringen att det finns starka skäl att hålla uppgifter om påföljder och uppgifter om misstankar åtskilda och att en uppdelning skulle göras genom att person- och belastningsregistret skulle ersättas av ett belastningsregister, i vilket endast påföljder och liknande skulle tas in, och ett misstankeregister. Riksdagen, som vid flera tillfällen tidigare uttalat sig för en sådan uppdelning, godkände regeringens förslag (bet. 1994/95:JuU21, rskr. 1994/95:378).

Genom införandet av lagen (1998:620) om belastningsregister och av lagen (1998:621) om misstankeregister genomfördes uppdelningen.

Belastningsregistret

Enligt 1 § lagen om belastningsregister ska Rikspolisstyrelsen föra ett rikstäckande belastningsregister. Rikspolisstyrelsen är personuppgiftsansvarig för registret.

Ändamålet med belastningsregistret är att ge information om sådana belastningsuppgifter som behövs i verksamhet hos polismyndigheter, Skatteverket, Tullverket och Kustbevakningen för att förebygga, upptäcka och utreda brott, hos åklagarmyndigheter för beslut om förundersökning och åtal och vid utfärdande av strafföreläggganden samt hos allmänna domstolar för val av påföljd och straffmätning. Uppgifter i registret ska också få användas av polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning och annan prövning som anges i lag eller förordning samt för att lämna uppgifter till enskilda om det är av särskild betydelse i den enskildes verksamhet. I lagen om belastningsregister bemyndigas regeringen att föreskriva att en myndighet får ha direktåtkomst till belastningsregistret.

Alla påföljder för brott ska registreras i belastningsregistret. Registret innehåller uppgifter om cirka 1 400 000 personer och cirka 2 900 000 noteringar om påföljder. De allra flesta av dessa noteringar avser bötespåföljder som fastställts genom föreläggande av ordningsbot.

Belastningsregistret ska vidare innehålla uppgifter om den som har ålagts förvandlingsstraff för böter, den som med tillämpning av 30 kap. 6 § brottsbalken har förklarats fri från påföljd och den som har meddelats besöksförbud. Vissa uppgifter om den som är dömd i utlandet ska också registreras.

Skyddet för den personliga integriteten kommer bl.a. till uttryck i begränsningar när det gäller utlämnande av uppgifter ur belastningsregistret. För registret gäller enligt 35 kap. 3 § offentlighets- och sekretesslagen (2009:400) absolut sekretess, vilket innebär att uppgifter endast får lämnas ut enligt vad som är särskilt föreskrivet. Domstolarna och de

myndigheter för vilkas verksamhet registret förs har rätt att få ut de uppgifter som är nödvändiga för att de ska kunna bedriva sin verksamhet. Vidare har den registrerade alltid rätt att få ut de uppgifter som finns registrerade om honom eller henne. Andra enskilda har rätt att i den utsträckning som regeringen föreskriver få ut uppgifter om andra personer ur registret, om det behövs för att pröva en fråga om anställning eller uppdrag i en verksamhet som avser vård eller som är av betydelse för att förebygga eller beivra brott. Vidare får uppgifter i vissa fall lämnas till utländska myndigheter och till myndigheter som för statistik.

Uppgifter i belastningsregistret gallras när förutsättningarna för registrering inte längre föreligger, t.ex. om den registrerade blir frikänd efter överklagande eller om en ordningsbot undanröjs. Vid frikännande dom plockas den tidigare domen bort direkt. Uppgifter ur belastningsregistret gallras vidare när viss tid förflutit, i de flesta situationer efter tio år. Uppgifter om bötespåföljd gallras dock efter fem år.

Personuppgiftslagens bestämmelser om rättelse och skadestånd gäller för behandlingen av personuppgifter i registret.

Regeringen bemyndigas i lagen om belastningsregister att utfärda föreskrifter om registrets närmare innehåll. Det kan bl.a. gälla uppgifter om utvisning, intagning i eller utskrivning från sjukvårdsinrättning av den som av domstol överlämnats till psykiatrisk vård samt uppgifter om resning.

Misstankeregistret

Enligt 1 § lagen om misstankeregister ska Rikspolisstyrelsen föra ett rikstäckande register med uppgifter om dem som är skäligen misstänkta för brott. Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Misstankeregistret ska föras för att underlätta tillgången till sådana uppgifter om skälig misstanke om brott som behövs i verksamhet hos polismyndigheter, Skatteverket, Tullverket och Kustbevakningen för att samordna förundersökningar mot en misstänkt person och för att förebygga, upptäcka och utreda brott samt hos åklagarmyndigheter för beslut om förundersökning och åtal. Registret får även användas av polismyndigheter och andra myndigheter som ska utföra lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning. Slutligen får registret användas för att till enskild lämna uppgift som är av särskild betydelse i dennes verksamhet.

Misstankeregistret innehåller uppgifter om den som har fyllt 15 år och som är skäligen misstänkt antingen för något brott mot brottsbalken eller för något annat brott för vilket svårare straff än böter är föreskrivet. Uppgifter förs också in om den som är skäligen misstänkt för ett motsvarande brott utomlands, om frågan om lagföring för brottet ska avgöras i Sverige. Registret innehåller vidare uppgifter om den mot vilken det har inletts utredning om förvandling av böter och om den som begärts överlämnad eller utlämnad för brott.

De myndigheter för vars räkning registret förs samt domstolarna har rätt att få uppgifter ur registret. Regeringen får föreskriva att andra myndigheter ska få uppgifter ur registret för vissa slag av ärenden eller för

särskilt fall. Uppgifter ur registret ska vidare i viss utsträckning kunna lämnas till myndigheter och organisationer utomlands.

Det finns ungefär 100 000 personer registrerade i misstankeregistret och omkring 300 000 uppgifter om brottsmisstankar i registret.

Uppgifter i misstankeregistret gallras om en förundersökning har avslutats utan att åtal har väckts med anledning av misstanken, om åtal har lagts ned eller om dom eller beslut angående misstanken har vunnit laga kraft.

Personuppgiftslagens bestämmelser om rättelse och skadestånd gäller för behandling av uppgifter i misstankeregistret.

Schengens informationssystem

Sverige är anslutet till Schengensamarbetet (prop. 1997/98:42, bet. 1997/98:JuU15, rskr. 1997/98:121). Schengensamarbetet bygger på två grundtankar. Den första är den fria rörligheten för personer, i den betydelsen att någon personkontroll vid nationsgränserna mellan Schengenstaterna inte ska förekomma. Den andra är att kampen mot internationell kriminalitet och illegal invandring ska stärkas.

Ett hjälpmedel i detta sammanhang är dataregistret Schengens informationssystem (SIS). SIS består av ett nationellt register för varje Schengenstat och en central teknisk stödfunktion, som är gemensam för Schengenländerna. Lagen (2000:344) om Schengens informationssystem innehåller regler om behandling av personuppgifter i den svenska enheten. Det register som är den svenska enheten i SIS förs av Rikspolisstyrelsen, som också är personuppgiftsansvarig. Registret är anslutet till den centrala enheten i SIS.

Varje Schengenstats nationella enhet innehåller uppgifter som är identiska med uppgifterna i de övriga ländernas nationella enheter.

Registret är ett hjälpmedel för Schengenstaterna att göra framställningar för att främja samarbete som avser polisiära och rättsliga frågor samt frågor om inresa och uppehållstillstånd. Det är uppbyggt som ett spanings- och efterlysningshjälpmedel. I SIS-registret kan varje Schengenstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersökta med en begäran om att en viss åtgärd ska vidtas när en efterlyst person eller ett efterlyst fordon påträffas. Uppgifterna i SIS-registret består av identifieringsuppgifter för registrerade personer. och föremål. De kompletterande uppgifter som behövs, för att ett land som har påträffat en efterlyst person eller ett efterlyst föremål ska kunna verkställa en begärd åtgärd, lämnas över först när det blir aktuellt i varje enskilt fall genom direkt kontakt mellan de berörda länderna.

Lagen om SIS innehåller bestämmelser om vilka framställningar som får föras in i registret. I lagen regleras också vilka personuppgifter som får föras in i registret, vem som får använda uppgifter ur det och ett förbud mot att använda uppgifter för annat ändamål än det som uppgiften registrerats för. I registret finns beträffande personer uppgift om namn, särskilda bestående fysiska kännetecken, födelsedatum och födelseort, kön, medborgarskap samt om personen är beväpnad eller kan tillgripa våld. Vidare registreras syftet med framställningen samt begärd åtgärd. Registret innehåller endast uppgifter som har behandlats av behöriga

myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning. Uppgifter registreras av Rikspolisstyrelsen endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen, polisdatalagen eller annan svensk författning. Känsliga personuppgifter registreras inte.

Uppgifterna i registret gallras senast ett, tre, fem eller tio år efter registreringen. Det tillämpas olika gallringstider för olika slag av uppgifter.

I lagen med tillhörande förordning anges vilka myndigheter som har rätt att ha direktåtkomst till registret.

Vapenregister

I 2 kap. vapenlagen (1996:67) finns bestämmelser om lokala och centrala vapenregister. Enligt 2 kap. 20 § vapenlagen ska vapenregistren ha till ändamål att ge information om sådana uppgifter som behövs för att förebygga, upptäcka och utreda brott med anknytning till skjutvapen samt underlätta handläggningen av frågor om tillstånd enligt vapenlagen. Rikspolisstyrelsen för centrala register över vapeninnehavare, vapen och vapenhandlare medan varje polismyndighet för ett lokalt vapenregister över tillståndspliktiga vapeninnehav. De centrala vapenregistren får av säkerhetsskäl inte samköras med varandra.

De lokala vapenregistren innehåller all information som krävs för polismyndighetens vapenärendehantering, såsom ansökan, uppgifter som kommer fram under handläggningen samt polismyndighetens beslut. Vilka uppgifter en ansökan ska innehålla regleras i vapenförordningen (1996:70) .

Det centrala vapeninnehavarregistret innehåller uppgifter om personer och organisationer som meddelats tillstånd att inneha vapen eller ammunition.

Det centrala vapenregistret innehåller uppgifter om de skjutvapen för vilka tillstånd till innehav har meddelats, såsom tillståndsnummer, vapentyp, fabrikat, modell, tillverkningsnummer m.m. Det innehåller också uppgifter om skjutvapen som upphittats eller anmälts stulna eller försvunna.

Speciella vapenregistret är ett register över stulna och försvunna vapen. Registret innehåller huvudsakligen indirekta personuppgifter i form av polisanmälans diarienummer. I registret förekommer personnummer endast om vapnet har märkts med ett sådant nummer.

I vapenhandlarregistret registreras bl.a. uppgifter om organisationsnummer, namn, adress, tillståndsnummer etc. på de fysiska eller juridiska personer som har tillstånd att driva handel med skjutvapen eller att ta emot skjutvapen för översyn eller reparation.

Passagerarregister

Enligt lagen (2006:444) om passagerarregister ska Rikspolisstyrelsen föra ett register över sådana passagerare som avses i 9 kap. 3 a § utlänningslagen (2005:716). Ändamålet med registret är att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som inte

tillhör EU och inte heller har träffat avtal om samarbete enligt Schengenkonventionen med konventionsstaterna.

Arbetet med att införa ett datoriserat passagerarregister är kraftigt försenat. I avvaktan på att ett datoriserat register kan tas i bruk används manuella rutiner.

Ordningsbotsregistret

Rikspolisstyrelsen för, med stöd av förordningen (1997:903) om register över förelägganden av ordningsbot, ett särskilt register över alla ordningsbotsförelägganden. Registret omfattar även de förelägganden som beslutas inom Tullverket och Kustbevakningen. Registret får användas för handläggning, uppbörd, och underrättelser till myndigheter samt för tillsyn, planering, uppföljning och framställning av statistik. Rikspolisstyrelsen är personuppgiftsansvarig för registret, medan polismyndigheterna, Tullverket och Kustbevakningen är personuppgiftsansvariga för uppgifterna i de ärenden som handläggs där. Registret får bl.a. innehålla uppgifter om fysiska personers namn, adress och personnummer, den brottsliga gärningen, förelagd ordningsbot, godkännande samt beslut av polisman, åklagare, tulltjänsteman, kustbevakningstjänsteman och domstol. I förordningen regleras sambearbetning och utlämnande av uppgifter i registret samt sökbegränsningar och gallring.

Register över uppbörd i ärenden om strafföreläggande

Förordningen (1997:902) om register över strafförelägganden innehåller bestämmelser om vilka register som får föras i ärenden om strafförelägganden. Enligt 4 § får Rikspolisstyrelsen föra ett register över uppbörd i ärenden om strafförelägganden. Uppbördsregistret får användas i ärenden om strafföreläggande för uppbörd enligt bötesverkställighetslagen (1979:189) samt för tillsyn, planering, uppföljning och framställning av statistik. Rikspolisstyrelsen är personuppgiftsansvarig för registret. Uppbördsregistret får bl.a. innehålla åklagarens namn och titel, den misstänktes eller den förelagdes namn och personuppgifter, uppgifter om målsäganden, brottsrubricering, gärningsbeskrivning och lagrum, påföljd, särskild rättsverkan och enskilt anspråk, den misstänktes eller den förelagdes inställning till föreläggandet, beslut av åklagare och domstol, uppgifter om ärendets handläggning i övrigt samt uppgifter om uppbörd av böter. I förordningen regleras även sambearbetning och utlämnande av uppgifter i registret samt sökbegränsningar och gallring.