

Passdatalag

– en ny lag som kompletterar
EU:s dataskyddsförordning

Ds 2019:5



Regeringskansliet
Justitiedepartementet

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

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.

Svara på remiss – hur och varför

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

En kort handledning för dem som ska svara på remiss.

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

Omslag: Regeringskansliets standard

Tryck: Elanders Sverige AB, Stockholm 2019

ISBN 978-91-38-24917-8

ISSN 0284-6012

Innehåll

Sammanfattning	7
1 Författningsförslag	11
1.1 Förslag till passdatalag	11
1.2 Förslag till passdataförordning	17
1.3 Förslag till lag om ändring i passlagen (1978:302).....	20
1.4 Förslag till förordning om ändring i passförordningen (1979:664).....	22
1.5 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).....	25
1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)	26
2 Promemorians bakgrund	29
3 Passverksamheten	31
3.1 Passverksamhet i teori och praktik	31
3.2 Regler om pass och passhandläggning	32
3.2.1 Reglerna i ljuset av grundlagen	32
3.2.2 Passlagen och anslutande föreskrifter	33
3.2.3 EU-regler om säkerhetsdetaljer.....	33
3.2.4 Pass utfärdas av flera myndigheter	34
3.2.5 Vanliga pass och särskilda pass	35
3.2.6 Passhandläggningens olika delar.....	37
3.2.7 Passkyldighet och passkontroll	42

3.3	Myndigheternas verksamhet i praktiken.....	43
3.3.1	En särskild uppgift för Polismyndigheten.....	43
3.3.2	Ambassaderna och konsulaten.....	43
3.3.3	Protokollet inom Utrikesdepartementet.....	44
3.3.4	Passverksamheten är datoriserad.....	45
3.3.5	Handläggningen i RES och RES-UM.....	47
3.4	Personuppgifter och sekretess.....	50
3.4.1	Vad är en personuppgift?.....	50
3.4.2	Personuppgifter i passärenden.....	50
3.4.3	Personuppgifter i Polismyndighetens register.....	52
3.4.4	Sekretess i passverksamheten.....	54
4	Regelverket om dataskydd.....	57
4.1	En översikt över regelverket.....	57
4.2	Det grundläggande integritetsskyddet.....	58
4.2.1	Överenskommelser inom FN och OECD.....	58
4.2.2	Europarådets konventioner och EU-stadgan.....	59
4.2.3	Regeringsformens integritetsskydd.....	61
4.3	Reglerna om personuppgiftsbehandling.....	61
4.3.1	Tidigare gällde personuppgiftslagen.....	61
4.3.2	Dataskyddsreformen innebär nya regler.....	62
4.3.3	Dataskyddsförordningens regelverk.....	63
4.3.4	Brottsdatalagens regelverk.....	67
4.4	Särskilda regler för passverksamheten.....	68
4.4.1	Ingen särskild registerförfattning.....	68
4.4.2	Bestämmelser om Polismyndighetens register.....	69
4.4.3	Bestämmelser om biometriska data.....	69
5	En passdatalag bör införas.....	71
5.1	Frågor som behöver övervägas.....	71
5.2	Brottsdatalagen är inte tillämplig.....	72
5.3	Dataskyddsförordningen är tillämplig.....	77
5.4	Personuppgiftsbehandlingen är laglig.....	78
5.5	Närmare regler är tillåtna och behövs.....	81

5.6	Reglerna bör meddelas genom lag.....	86
5.7	En ny registerförfattning bör införas	91
5.8	Något om statliga identitetskort.....	92
6	Passdatalagens innehåll.....	95
6.1	Syfte och utgångspunkter.....	95
6.2	Definitioner av ord och uttryck.....	96
6.3	Avgränsning av tillämpningsområdet	97
6.4	Förhållandet till andra regler om dataskydd.....	101
6.5	Ansvaret för behandlingen	102
6.6	När personuppgifter får behandlas	107
6.6.1	Ändamålsbestämmelser bör införas	107
6.6.2	Passhandläggning som primärt ändamål	110
6.6.3	Gränskontroll som sekundärt ändamål	112
6.6.4	Brottsbekämpning som sekundärt ändamål.....	113
6.6.5	Uppgiftslämnande som sekundärt ändamål.....	116
6.6.6	Övriga sekundära ändamål	118
6.7	Den registrerades rättigheter.....	119
6.8	Vissa säkerhetsåtgärder.....	126
6.9	Register i passverksamheten.....	128
6.9.1	Polismyndigheten bör ha två register.....	128
6.9.2	Vad bör passregistret få innehålla?	130
6.9.3	Vad bör passtillståndsregistret få innehålla?	132
6.10	Integritetskänsliga uppgifter	133
6.10.1	Flera frågor behöver analyseras	133
6.10.2	Regelverket om känsliga personuppgifter.....	134
6.10.3	Känsliga personuppgifter i allmänhet.....	135
6.10.4	Biometrisk jämförelse av ansiktsbilder.....	141
6.10.5	Lagöverträdelser och personnummer.....	151
6.11	Sökbegränsningar i verksamheten.....	153
6.12	Elektroniskt utlämnande av personuppgifter.....	157
6.12.1	Elektroniskt utlämnande i allmänhet	157

6.12.2	Elektroniskt utlämnande genom direktåtkomst	160
6.13	Sekretessbrytande uppgiftsskyldighet.....	167
6.14	Bevarande och gallring	171
6.15	Tillsyn, överklagande och skadestånd	181
7	Sekretess för biometriska uppgifter.....	183
8	Ikraftträdande- och övergångsbestämmelser	187
9	Konsekvenser av förslagen	189
10	Författningskommentar	195
10.1	Förslaget till passdatalag	195
10.2	Förslaget till lag om ändring i passlagen (1978:302)	216
10.3	Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)	217
Bilaga 1	Sammanfattning Ds 2015:44.....	219
Bilaga 2	Författningsförslag i fråga om pass i Ds 2015:44	221
Bilaga 3	Förteckning över remissinstanserna (Ds 2015:44)	233

Sammanfattning

Pass och personuppgifter

Alla svenska medborgare har som huvudregel rätt att få ett pass. Ett giltigt pass är i princip en förutsättning för att få resa ut ur landet.

Varje år ansöker över en och en halv miljon svenskar om pass. Passärenden handläggs av passmyndigheter. Polismyndigheten är passmyndighet inom landet medan vissa ambassader och konsulat fungerar som passmyndigheter i utlandet. Vissa kategorier av pass, diplomatpass och tjänstepass, utfärdas av Utrikesdepartementet.

När en person ansöker om pass samlar myndigheterna in viss information. Det handlar om namn och personnummer men också om ansiktsbild, fingeravtryck och andra uppgifter. Flera av dessa uppgifter sparas i Polismyndighetens passregister. Detta innehåller data om en stor del av befolkningen och utgör en viktig källa till information både i passverksamheten och i andra sammanhang.

Problemet med dagens regelverk

På många områden finns det särskilda registerförfattningar som preciserar hur myndigheter får behandla personuppgifter i en viss verksamhet. Det kan handla om vilka register som ska finnas, hur olika uppgifter får användas och hur länge information får bevaras.

För passverksamheten finns det inte någon registerförfattning. Passlagstiftningen i sig innehåller bara några få bestämmelser som handlar om hur personuppgifter får behandlas. Det framgår att det ska finnas ett passregister men det sägs ingenting om vad det får innehålla, hur informationen i registret får användas eller hur länge den får bevaras. Även i övrigt saknas det närmare bestämmelser om hur personuppgifter får behandlas inom passverksamheten.

Avsaknaden av närmare bestämmelser har kritiserats av Lagrådet och är problematisk både från ett integritetsperspektiv och från ett verksamhetsperspektiv. Både den enskilde och myndigheterna kan uppfatta det som oklart vilka personuppgifter som över huvud taget får samlas in, vilka uppgifter som får sparas i passregistret, vilka sökningar som får göras, på vilka sätt uppgifter får lämnas ut och hur länge uppgifter får bevaras. Det kan också framstå som oklart hur den information som finns i passverksamheten får användas. Är det t.ex. tillåtet att använda ett passfoto för att utreda ett brott?

Regelverket har utretts tidigare

Frågan om en särskild registerförfattning för passverksamheten har utretts tidigare. I promemorian Passdatalag (Ds 2015:44) föreslogs en passdatalag som skulle reglera behandlingen av personuppgifter i passverksamheten. På grund av den stora dataskyddsreform som beslutades inom EU under våren 2016 har förslagen i promemorian emellertid inte kunnat genomföras. Nya analyser och bedömningar har krävts och saken utreds därför på nytt i denna promemoria.

Nu gäller dataskyddsförordningen

Dataskyddsreformen består av två nya regelverk. Det första är en allmän dataskyddsförordning, som i vardagligt tal brukar kallas för GDPR (eng. General Data Protection Regulation). Det andra är ett direktiv som gäller när vissa myndigheter behandlar personuppgifter i syfte att bekämpa eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Den behandling av personuppgifter som passmyndigheterna och Utrikesdepartementet utför i passverksamheten syftar inte till att bekämpa eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Direktivet är därför inte tillämpligt. I stället gäller dataskyddsförordningen.

Dataskyddsförordningen är bindande och direkt tillämplig i alla medlemsstater. Den innehåller grundläggande principer som gäller vid all behandling av personuppgifter. Den innehåller också en rad bestämmelser om den registrerades rättigheter och om skyldigheter för den som behandlar personuppgifter. Passmyndigheterna och

Utrikesdepartementet ska följa dataskyddsförordningen när de behandlar personuppgifter i passverksamheten.

En kompletterande lag föreslås

Dataskyddsförordningen gäller generellt för olika samhällssektorer och är inte anpassad särskilt för passverksamheten. I vissa avseenden förutsätter eller tillåter förordningen att medlemsstaterna inför kompletterande bestämmelser i nationell rätt. Det finns därför ett utrymme för nationella bestämmelser som preciserar förordningen. Det finns också ett utrymme för vissa undantag från förordningen.

För att förtydliga vad som gäller när personuppgifter behandlas i passverksamheten föreslås en särskild registerförfattning i form av en passdatalag. Lagen ska komplettera dataskyddsförordningen och bidra till att myndigheterna kan behandla personuppgifter på ett ändamålsenligt sätt samtidigt som människor skyddas mot att deras personliga integritet kränks. Det föreslås att bl.a. följande ska gälla:

- Personuppgifter ska få samlas in bara om det är nödvändigt för handläggning av passärenden. Personuppgifter som har samlats in för detta ändamål ska dock få användas även för vissa andra ändamål, t.ex. gränskontroll och brottsbekämpning.
- Passmyndigheterna och Utrikesdepartementet ska ansvara för den behandling av personuppgifter som respektive myndighet utför. Polismyndigheten ska ansvara för passregistret.
- Den interna tillgången till personuppgifter inom myndigheterna ska begränsas till det som varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.
- Passregistret ska bara få innehålla uppgifter om personer som är eller har varit parter i passärenden. Bara vissa uppgifter, som räknas upp i lagen, ska få registreras. Uppgifter och handlingar i passregistret ska i princip raderas efter tio år.
- Känsliga personuppgifter ska som huvudregel få behandlas bara om det är absolut nödvändigt för ändamålet med behandlingen.
- Vissa typer av sökningar och sökbegrepp ska vara förbjudna. Den ansiktsbild som tas i samband med en passansökan ska dock

kunna jämföras biometriskt med bilderna i passregistret. Vissa biometriska uppgifter ska därför få lagras i passregistret.

- De fingeravtryck som lämnas i samband med en passansökan ska liksom i dag omedelbart förstöras när passet har lämnats ut.
- Personuppgifter ska få lämnas ut elektroniskt bara efter en särskild prövning. Vissa möjligheter till direktåtkomst ska finnas.

Lagen ska enligt förslaget kompletteras av en passdataförordning med vissa verkställighetsföreskrifter och bemyndiganden m.m. För att säkerställa att det finns ett sekretesskydd för biometriska uppgifter föreslås även en ändring i sekretesslagstiftningen.

De nya bestämmelserna föreslås träda i kraft den 1 juli 2020.

Konsekvenserna av den nya lagen

Den nya lagen bedöms leda till ett starkare skydd för den enskildes personliga integritet. Lagen preciserar dataskyddsförordningen och förtydligar hur personuppgifter får behandlas i passverksamheten. I flera avseenden föreslås ett starkare integritetsskydd än vad dataskyddsförordningen kräver. En särskild registerförfattning med tydliga bestämmelser skapar också goda förutsättningar för tillsyn.

Förslagen bedöms även bidra till att motverka brottslighet och missbruk av identitetshandlingar. Den nya lagen säkerställer att personuppgifter i passverksamheten kan användas för att bekämpa brott. Möjligheten att på teknisk väg jämföra ansiktsbilder vid en passansökan motverkar att pass utfärdas på felaktiga grunder.

För de myndigheter som handlägger passärenden bedöms lagen bidra till en effektiv verksamhet, med tydliga förutsättningar för behandlingen av personuppgifter. De kostnader som förslagen kan ge upphov till ryms inom myndigheternas befintliga anslag.

1 Författningsförslag

1.1 Förslag till passdatalag

Härigenom föreskrivs följande.

Syftet med lagen

1 § Syftet med denna lag är att personuppgifter ska kunna behandlas på ett ändamålsenligt sätt i passverksamheten, samtidigt som människor skyddas mot att deras personliga integritet kränks vid sådan behandling.

Ord och uttryck i lagen

2 § Med passverksamhet avses i denna lag verksamhet enligt passlagen (1978:302). Övriga ord och uttryck som används i lagen har samma betydelse som i passlagen.

Lagens tillämpningsområde

3 § Denna lag gäller när passmyndigheterna och Regeringskansliet (Utrikesdepartementet) behandlar personuppgifter i passverksamheten.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Förhållandet till annan reglering

4 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

5 § Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Personuppgiftsansvar

6 § Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) är personuppgiftsansvariga för den behandling av personuppgifter som respektive myndighet utför.

Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i passregistret och passstillståndsregistret.

Ändamålen med behandlingen

7 § Personuppgifter får behandlas om det är nödvändigt för handläggning av ärenden om pass.

8 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för gränskontroll.

9 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

10 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

11 § Personuppgifter som behandlas enligt 7 § får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Rätten att göra invändningar

12 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Säkerhetsåtgärder

13 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

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

1. närmare föreskrifter om tillgången till personuppgifter, och
2. ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Register i passverksamheten

14 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett passregister och ett passtillståndsregister.

15 § Passregistret får endast innehålla uppgifter om en person som är eller har varit part i ett ärende om pass. Passregistret får i fråga om en sådan person endast innehålla följande uppgifter:

1. namn,
2. person- eller samordningsnummer,
3. medborgarskap,
4. födelseort,

5. kön,
6. längd,
7. ansiktsbilder som har tagits vid passansökningar,
8. biometriska uppgifter som har tagits fram ur ansiktsbilderna,
9. namnteckningar som har lämnats vid passansökningar,
10. uppgifter i handlingar som har kommit in eller upprättats, och
11. uppgifter om pass och om handläggningen av ärenden om pass.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter som får behandlas med stöd av första stycket.

16 § Passtillståndsregistret får endast innehålla de uppgifter som är nödvändiga för att man ska kunna avgöra om det krävs passtillstånd för en person enligt 20 § 1 eller 3 passlagen (1978:302).

Behandling av känsliga personuppgifter

17 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas i följande fall:

1. i passregistret när det är tillåtet enligt 15 §,
2. i passtillståndsregistret när det är tillåtet enligt 16 §, och
3. vid sökning som är tillåten enligt 19 § andra stycket.

Sökbegränsningar

18 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelse som avses i artikel 10 i EU:s dataskyddsförordning.

19 § Det är förbjudet att använda fingeravtryck och ansiktsbilder samt biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder som sökbegrepp.

Trots förbudet får den ansiktsbild som tas vid en passansökan och de biometriska uppgifter som tas fram ur ansiktsbilden användas vid

sökning i passregistret, för att kontrollera sökandens identitet och innehav av pass i samband med passansökan.

20 § Sökförbudet i 18 § och 19 § första stycket gäller även vid sökningar i passregistret och passtillståndsregistret för andra ändamål än handläggning av ärenden om pass.

Uppgiftsskyldighet

21 § En passmyndighet eller Regeringskansliet (Utrikesdepartementet) har vid direktåtkomst enligt 25 § första stycket rätt att ta del av personuppgifter som en annan passmyndighet eller Regeringskansliet (Utrikesdepartementet) behandlar.

Säkerhetspolisen har vid direktåtkomst enligt 25 § andra stycket rätt att ta del av personuppgifter som behandlas i passregistret.

22 § Polismyndigheten ska på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen, Ekobrottsmyndigheten, en svensk ambassad, ett svenskt lönat konsulat, Försvarsmakten, Kustbevakningen, Tullverket, Skatteverket eller Kronofogdemyndigheten.

Elektroniskt utlämnande av personuppgifter

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

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 24 och 25 §§.

24 § Uppgift om ett pass giltighet får lämnas ut genom direktåtkomst.

25 § Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) får medge varandra direktåtkomst till personuppgifter.

Säkerhetspolisen får medges direktåtkomst till personuppgifter i passregistret. I sådant fall gäller sökförbudet i 18 § och 19 § första stycket.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheten att medge direktåtkomst enligt första och andra styckena.

Bevarande och gallring

26 § Uppgifter och handlingar i passregistret ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades.

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

1. att uppgifter och handlingar får bevaras för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i första stycket, och

2. avskiljande och begränsningar av åtkomsten till uppgifter och handlingar som bevaras för sådana ändamål som anges i 1.

27 § De fingeravtryck som tas vid en passansökan och de biometriskt uppgifter som tas fram ur fingeravtrycken ska omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.

Denna lag träder i kraft den 1 juli 2020.

1.2 Förslag till passdataförordning

Härigenom föreskrivs följande.

Allmän bestämmelse

1 § I denna förordning finns kompletterande föreskrifter till passdatalagen (2020:000).

Säkerhetsåtgärder

2 § Polismyndigheten får meddela närmare föreskrifter om tillgången till personuppgifter inom myndigheten.

Polismyndigheten får meddela föreskrifter om andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten.

3 § Regeringskansliet (Utrikesdepartementet) får meddela närmare föreskrifter om tillgången till personuppgifter inom myndigheten och passmyndigheter utom riket.

Regeringskansliet (Utrikesdepartementet) får meddela föreskrifter om andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten och passmyndigheter utom riket.

Register i passverksamheten

4 § Följande uppgifter får behandlas i passregistret med stöd av 15 § första stycket 11 passdatalagen (2020:000):

1. pass som har utfärdats,
2. ärendenummer,
3. beslut som har fattats,
4. andra handläggningsåtgärder, och
5. kontaktuppgifter.

Elektroniskt utlämnande av personuppgifter

5 § Passmyndigheternas och Regeringskansliets (Utrikesdepartementet) direktåtkomst enligt 25 § första stycket passdatalagen (2020:000) ska begränsas till de personuppgifter som varje myndighet behöver för att handlägga ärenden om pass.

6 § Säkerhetspolisens direktåtkomst enligt 25 § andra stycket passdatalagen (2020:000) ska begränsas till de personuppgifter som Säkerhetspolisen behöver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Bevarande och gallring

7 § Riksarkivet får meddela föreskrifter om att uppgifter och handlingar som ska gallras enligt 26 § första stycket passdatalagen (2020:000) får bevaras under längre tid för arkivändamål av allmänt intresse och för vetenskapliga, statistiska eller historiska ändamål. Innan sådana föreskrifter meddelas ska Polismyndigheten och Regeringskansliet (Utrikesdepartementet) ges tillfälle att yttra sig.

8 § Uppgifter och handlingar som bevaras med stöd av sådana föreskrifter som avses i 7 § ska avskiljas från den löpande passverksamheten. Åtkomsten till avskilda uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Rätt att kontrollera information i passet

9 § En passinnehavare har rätt att hos en passmyndighet kontrollera den information som har sparats i lagringsmediet i passet.

Rätt att meddela föreskrifter

10 § Polismyndigheten får meddela ytterligare föreskrifter om verkställigheten av passdatalagen (2020:000) och denna förordning inom Polismyndighetens ansvarsområde.

11 § Regeringskansliet (Utrikesdepartementet) får meddela ytterligare föreskrifter om verkställigheten av passdatalagen (2020:000) och denna förordning inom myndighetens och utlandsmyndigheternas ansvarsområden.

12 § Innan Polismyndigheten eller Regeringskansliet (Utrikesdepartementet) meddelar föreskrifter med stöd av denna förordning ska Datainspektionen ges tillfälle att yttra sig.

Denna förordning träder i kraft den 1 juli 2020.

1.3 Förslag till lag om ändring i passlagen (1978:302)

Härigenom föreskrivs i fråga om passlagen (1978:302)¹

dels att 6 b § ska upphöra att gälla,

dels att 5 a och 6 a §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

5 a §²

Polismyndigheten ska övervaka att bestämmelserna i 5 § följs.

Den som enligt 5 § ska medföra pass ska på begäran

1. överlämna passet till en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Kustbevakningen, Tullverket eller Migrationsverket, och

2. låta en befattningshavare enligt 1 ta passinnehavarens fingeravtryck och en bild i digitalt format av hans eller hennes ansikte för kontroll av att dessa motsvarar de fingeravtryck och den ansiktsbild som finns sparade i passet.

Den som enligt 5 § i stället medför ett identitetskort utfärdat av en passmyndighet ska på begäran

1. överlämna identitetskortet till en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Kustbevakningen, Tullverket eller Migrationsverket, och

2. låta en befattningshavare enligt 1 ta en bild i digitalt format av hans eller hennes ansikte för kontroll av att denna motsvarar den ansiktsbild som finns sparad i identitetskortet.

När en kontroll enligt andra stycket 2 eller tredje stycket 2 har genomförts, ska fingeravtrycken och ansiktsbilden samt de biometriska *data* som då har tagits fram omedelbart förstöras.

När en kontroll enligt andra stycket 2 eller tredje stycket 2 har genomförts, ska fingeravtrycken och ansiktsbilden samt de biometriska *uppgifter* som då har tagits fram omedelbart förstöras.

¹ Senaste lydelse av 6 b § 2009:387.

² Senaste lydelse 2015:336.

6 a §³

Fingeravtrycken och ansiktsbilden enligt 6 § andra stycket 1 ska sparas i ett lagringsmedium i passet.

Fingeravtrycken och de biometrisk data som tas fram ur dessa och ur ansiktsbilden ska omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.

Denna lag träder i kraft den 1 juli 2020.

³ Senaste lydelse 2009:387.

1.4 Förslag till förordning om ändring i passförordningen (1979:664)

Härigenom föreskrivs i fråga om passförordningen (1979:664)¹
dels att 22 a och 23 §§ ska upphöra att gälla,
dels att rubriken närmast före 23 § ska utgå,
dels att 19 och 24 §§ ska ha följande lydelse,
dels att det ska införas en ny paragraf, 24 a §, av följande lydelse,
dels att det närmast före 23 a § ska införas en ny rubrik som ska
 lyda ”Underrättelseskyldighet i vissa fall”.

Nuvarande lydelse

Föreslagen lydelse

19 §²

Anmälan av chefsöverläkare enligt 20 § 1 passlagen (1978:302) ska göras till Polismyndigheten. *Chefsöverläkaren ska återkalla anmälan om de omständigheter som har föranlett den inte längre finns.*

Anmälan av chefsöverläkare enligt 20 § 1 passlagen (1978:302) ska göras till Polismyndigheten.

Chefsöverläkaren ska återkalla anmälan om de omständigheter som har föranlett den inte längre finns.

Chefsöverläkaren ska underätta Polismyndigheten när den person som anmälan avser inte längre är intagen för sådan vård som anges i 20 § passlagen.

24 §³

Om det finns omständigheter som enligt 24 § första stycket passlagen (1978:302) bör medföra att framställning görs om att

Om det finns omständigheter som enligt 24 § första stycket passlagen (1978:302) bör medföra att framställning görs om att

¹ Senaste lydelse av
22 a § 2005:659
23 § 2014:1130
rubriken närmast före 23 § 1979:921.

² Senaste lydelse 2014:1130.

³ Senaste lydelse 2005:1000.

ett pass *skall* återkallas för den som avtjänar fängelsestraff eller står under övervakning efter dom på skyddstillsyn eller villkorlig frigivning från fängelse, *skall* Kriminalvården göra anmälan om det till övervakningsnämnden. På motsvarande sätt *skall* chefsöverläkare göra anmälan till Socialstyrelsen, om ett pass bör återkallas för en sådan patient som avses i 24 § andra stycket passlagen.

Framställning om passåterkallelse som har beslutats av en övervakningsnämnd eller Socialstyrelsen *skall*, sedan beslutet har *vunnit* laga kraft, översändas till passmyndigheten. Om det finns risk för att passinnehavaren reser ut ur landet innan beslutet har *vunnit* laga kraft, *skall* passmyndigheten omedelbart underrättas om beslutet. Det gäller också i fråga om en sådan framställning som avses i 25 § passlagen.

ett pass *ska* återkallas för den som avtjänar fängelsestraff eller står under övervakning efter dom på skyddstillsyn eller villkorlig frigivning från fängelse, *ska* Kriminalvården göra anmälan om det till övervakningsnämnden. På motsvarande sätt *ska* chefsöverläkare göra anmälan till Socialstyrelsen, om ett pass bör återkallas för en sådan patient som avses i 24 § andra stycket passlagen.

Framställning om passåterkallelse som har beslutats av en övervakningsnämnd eller Socialstyrelsen *ska*, sedan beslutet har *fått* laga kraft, översändas till passmyndigheten *och, i förekommande fall, till den chefsöverläkare som har gjort anmälan enligt första stycket*. Om det finns risk för att passinnehavaren reser ut ur landet innan beslutet har *fått* laga kraft, *ska* passmyndigheten omedelbart underrättas om beslutet. Det gäller också i fråga om en sådan framställning som avses i 25 § passlagen.

24 a §

Om Socialstyrelsen har gjort en framställning om återkallelse av pass enligt 24 § andra stycket passlagen (1978:302) ska den chefsöverläkare som har gjort anmälan till Socialstyrelsen enligt 24 § första stycket underrätta Polismyndigheten när den person som

*anmälan avser inte längre är
intagen för sådan vård som anges i
20 § passlagen.*

Denna förordning träder i kraft den 1 juli 2020.

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

Härigenom föreskrivs att 22 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

22 kap.

1 §

Sekretess gäller för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs och uppgiften förekommer i verksamhet som avser

1. folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen, eller

2. förande av eller uttag ur sjömansregistret.

Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av *en* fotografisk bild av den enskilde, *och biometrisk uppgift som har tagits fram ur en sådan bild*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

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

Denna lag träder i kraft den 1 juli 2020.

1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att 6 § offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

6 §¹

Sekretess gäller i nedan angiven verksamhet, som avser registrering av betydande del av befolkningen, för

1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och

2. uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

Sekretess gäller i nedan angiven verksamhet, som avser registrering av *en* betydande del av befolkningen, för

1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och

2. uppgift i form av *en* fotografisk bild av den enskilde, *och biometrisk uppgift som har tagits fram ur en sådan bild*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

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

Verksamheten avser

centrala hundregistret

fastighetsregistret

kommunala fastighetsregister

passregister och register över nationella identitetskort

röstlängdsregister

Skatteverkets databas över identitetskort för folkbokförda i Sverige

Socialstyrelsens register över hälso- och sjukvårdspersonal

Statens tjänstepensionsverks pensionsregister

¹ Senaste lydelse 2014:1369.

Totalförsvarets rekryteringsmyndighets register över total-
försvarets personal
Transportstyrelsens vägtrafikregister

Denna förordning träder i kraft den 1 juli 2020.

2 Promemorians bakgrund

Den här promemorian handlar om behandling av personuppgifter i passverksamheten. Bakgrunden kan beskrivas på följande sätt.

Varje svensk medborgare har som huvudregel rätt att få ett pass. Den som vill ha ett pass ska ansöka om det hos en passmyndighet. Inom landet är Polismyndigheten passmyndighet. I utlandet är vissa ambassader och konsulat passmyndigheter. Vissa typer av pass utfärdas inte av passmyndigheterna utan av Utrikesdepartementet.

Vid sidan av pass kan svenska medborgare också få nationella identitetskort. Även dessa utfärdas av passmyndigheterna.

I verksamheten med pass och nationella identitetskort behandlas ett stort antal personuppgifter. Det handlar inte bara om namn och personnummer utan också om fotografier och fingeravtryck m.m. Många av uppgifterna lagras i Polismyndighetens register över pass och nationella identitetskort. Bestämmelserna om dessa register, och om behandlingen av personuppgifter i verksamheten i övrigt, har kritiserats för att vara ofullständiga och bristfälliga. Detta har ansetts otillfredsställande inte minst från ett integritetsskyddsperspektiv.

I juli 2014 fick en utredare i uppdrag att se över regleringen och vid behov föreslå nya eller ändrade bestämmelser för behandlingen av personuppgifter i verksamheten avseende pass och nationella identitetskort. Uppdraget redovisades i augusti 2015 i promemorian Passdatalag (Ds 2015:44). Promemorian innehöll en kartläggning av den personuppgiftsbehandling som förekommer i verksamheten och flera författningsförslag. När det gällde passverksamheten föreslogs att personuppgiftsbehandlingen skulle regleras i en passdatalag och en passdataförordning. Därutöver föreslog utredaren en förordning om behandling av personuppgifter i verksamhet avseende nationellt identitetskort. En sammanfattning av promemorian finns i *bilaga 1*. Promemorians författningsförslag i fråga om pass finns i *bilaga 2*.

Förslagen i promemorian remissbehandlades under 2015 och 2016. En förteckning över remissinstanserna finns i *bilaga 3*.

Samtidigt pågick inom Europeiska unionen (EU) ett arbete med en dataskyddsreform, dvs. en reform av unionens bestämmelser om personuppgiftsbehandling. Reformarbetet ledde bl.a. till en allmän dataskyddförordning, som började tillämpas den 25 maj 2018. Till följd av dataskyddsreformen har förutsättningarna för nationella regler om personuppgiftsbehandling förändrats. Förslagen i promemorian Passdatalag kan därför inte genomföras utan vidare analyser.

I den här promemorian görs, utifrån dataskyddsreformen, en ny genomgång av personuppgiftsbehandlingen i passverksamheten. Frågan är om det fortfarande behövs närmare regler på nationell nivå, genom en passdatalag eller på annat sätt, och om unionsrätten i sådana fall ger utrymme för det. Om personuppgiftsbehandlingen ska regleras närmare är frågan hur bestämmelserna bör utformas.

Behandlingen av personuppgifter i verksamheten med nationella identitetskort berörs inte närmare i promemorian. Skälet är att 2017 års ID-kortsutredning har föreslagit att förordningen (2005:661) om nationellt identitetskort ska upphävas och ersättas av regler om ett statligt identitetskort. Detta framgår av betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14). Utredningen har föreslagit särskilda regler om personuppgiftsbehandling när det gäller sådana identitetskort. Förslaget berörs kort i avsnitt 5.8.

3 Passverksamheten

3.1 Passverksamhet i teori och praktik

Det här kapitlet beskriver passverksamheten i stort. Det är fråga om att sätta in behandlingen av personuppgifter i ett sammanhang.

Bestämmelser om pass finns i första hand i passlagen (1978:302). En svensk medborgare får som huvudregel inte lämna landet utan pass. Pass utfärdas i form av vanligt pass eller särskilt pass. Ett vanligt pass är giltigt i fem år eller, om sökanden inte har fyllt tolv, tre år. Till de särskilda passen räknas bl.a. det provisoriska passet.

De myndigheter som utfärdar pass kallas för passmyndigheter. Polismyndigheten är passmyndighet inom landet medan vissa ambassader och konsulat fungerar som passmyndigheter i utlandet. Diplomats- och tjänstepass utfärdas av Utrikesdepartementet.

Den som vill ha ett pass ska vända sig till en passmyndighet med en ansökan. Sökanden ska inställa sig personligen. Han eller hon ska styrka sin identitet och sitt svenska medborgarskap och även låta myndigheten ta hans eller hennes fingeravtryck och ansiktsbild.

I vissa fall ska passansökan avslås. Det gäller bl.a. om sökanden är anhållen eller häktad. Det finns också situationer, bl.a. när sökanden avtjänar ett fängelsestraff eller är intagen för psykiatrisk tvångsvård, då pass inte får utfärdas utan ett särskilt tillstånd (passtillstånd).

Om pass utfärdas ska sökandens fingeravtryck och ansiktsbild sparas i ett lagringsmedium (ett chip) i passet. Ett utfärdat pass ska återkallas bl.a. om sökanden förlorar sitt svenska medborgarskap.

Det finns drygt åtta miljoner giltiga pass. Ungefär en och en halv miljon svenskar ansöker om pass varje år. Passhandläggningen är datoriserad och sker med stöd av Resehandlingssystemet (RES). Systemet fungerar också som ett passregister, som används både i passverksamheten och i vissa andra sammanhang. I RES finns även ett register över vissa personer som behöver ha passtillstånd.

Passmyndigheterna behandlar personuppgifter i sin verksamhet, både inom ramen för ärendehandläggningen och i sina register. Vissa känsligare uppgifter i verksamheten kan omfattas av sekretess.

Den fortsatta genomgången består av tre delar. Först lämnas en närmare beskrivning av reglerna om pass och passhandläggning, dvs. bestämmelserna i passlagen, passförordningen (1979:664) och vissa myndighetsföreskrifter. Därefter behandlas passmyndigheternas verksamhet i praktiken, bl.a. hur de använder sig av datorsystem. Avslutningsvis finns närmare information om vilka personuppgifter som behandlas i verksamheten och vilken sekretess som gäller.

3.2 Regler om pass och passhandläggning

3.2.1 Reglerna i ljuset av grundlagen

Bestämmelser om svenska pass har funnits länge. Ett viktigt inslag i regelverket har varit, och är fortfarande, ett principiellt förbud för svenska medborgare att lämna landet utan pass, dvs. ett passtvang eller en passkyldighet. Sedan slutet av 1970-talet är det emellertid inte längre straffbelagt att resa ut ur landet utan pass (jfr regeringens proposition med förslag till passlag, prop. 1977/78:156 s. 33 f.).

En fråga som har diskuterats är hur passtvangen förhåller sig till den grundlagsskyddade rörelsefriheten. Den innefattar en frihet för svenska medborgare både att förflytta sig inom landet och att lämna det (2 kap. 8 § regeringsformen). Friheten får begränsas under vissa förutsättningar men bara genom lag (2 kap. 20 § regeringsformen).

I förarbetena till regeringsformen uttalades att passtvangen var en klar begränsning av svenska medborgares rätt att lämna landet. Passkyldigheten skulle därför regleras i lag. Kravet på en reglering i lag ansågs gälla inte bara passtvangen i inskränkt mening utan även rätten att få ett pass (regeringens proposition med förslag till ny regeringsform och ny riksdagsordning m.m., prop. 1973:90 s. 241).

Den här tolkningen av regeringsformen var en utgångspunkt vid tillkomsten av passlagen. I förarbetena till lagen angavs att både passkyldigheten och rätten för svenska medborgare att få och behålla pass borde lagregleras. Samma sak ansågs gälla i fråga om förfarandet vid en passansökan och giltighetstiden för ett pass. När det gällde hinder mot pass angavs att en passvägran i sak innebar ett förbud mot att lämna landet och därför framstod som en begränsning av

medborgarnas rörelsefrihet. Man ansåg därför att även frågor om passhinder borde regleras i lag (prop. 1977/78:156 s. 10 och 15).

Passlagens regler ska alltså ses i ljuset av grundlagens skydd för rörelsefriheten. Passtvänet har ansetts inskränka den friheten.

3.2.2 Passlagen och anslutande föreskrifter

Den nuvarande passlagen trädde i kraft den 1 januari 1980. Lagen reglerar både passtvänet och rätten för svenska medborgare att få ett pass. Lagen innehåller också bestämmelser om bl.a. passansökan, hinder mot pass, giltighetstiden för pass och återkallelse av pass.

Passlagen gäller i allt väsentligt bara beträffande pass för svenska medborgare. Passföreskrifter i fråga om utländska medborgare finns i utlänningslagen (2005:716) och utlänningsförordningen (2006:97). Där framgår bl.a. att utländska medborgare som reser in i eller vistas i Sverige ska ha pass och att främlingspass kan utfärdas i vissa fall. Pass för utländska medborgare berörs inte i den här promemorian.

Vem som är svensk medborgare och därmed har rätt att få ett svenskt pass framgår inte av passlagen. Frågor om medborgarskap regleras i stället i lagen (2001:82) om svenskt medborgarskap.

Passlagen kompletteras i första hand av passförordningen, som innehåller närmare föreskrifter om handläggningen av passärenden. Därutöver finns det myndighetsföreskrifter om passverksamheten. För pass som utfärdas inom landet, av Polismyndigheten, gäller Polismyndighetens föreskrifter och allmänna råd (PMFS 2019:3) om pass och nationellt identitetskort. För pass som utfärdas av ambassader och konsulat gäller Regeringskansliets föreskrifter (UF 2009:9) om handläggningen av ärenden om pass, Europeiska unionens provisoriska resehandling och nationellt identitetskort. För pass som utfärdas inom Utrikesdepartementet gäller Regeringskansliets föreskrifter (UF 2018:1) om diplomat- och tjänstepass.

3.2.3 EU-regler om säkerhetsdetaljer

När det gäller säkerhetsdetaljer och biometriska kännetecken i pass finns det vissa bestämmelser på EU-nivå, nämligen i rådets förordning nr 2252/2004 av den 13 december 2004 om standarder

för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna samt i Europaparlamentets och rådets förordning (EG) nr 444/2009 av den 28 maj 2009 om ändring av rådets förordning (EG) nr 2252/2004.

Förordningarna är direkt tillämpliga i Sverige och innebär att pass med en giltighetstid på mer än tolv månader ska uppfylla vissa minimisäkerhetsstandarder. De ska bl.a. innehålla ett lagringsmedium med passinnehavarens ansiktsbild och fingeravtryck. Syftet med dessa bestämmelser är att öka säkerheten i passen. Inom EU finns det vidare vissa resolutioner om pass, som inte är bindande.

3.2.4 Pass utfärdas av flera myndigheter

Pass utfärdas av passmyndigheter (2 § passlagen). Polismyndigheten är passmyndighet inom landet. I utlandet fungerar vissa svenska beskickningar (ambassader) och konsulat som passmyndigheter.

Före passlagens tillkomst var länsstyrelserna passmyndigheter inom landet. De dåvarande polismyndigheterna utförde dock den passhinderutredning som krävdes. Det gick även att ansöka om pass hos en polismyndighet, som efter sin passhinderutredning lämnade över ärendet till länsstyrelsen för beslut. Det ansågs bl.a. av dessa skäl vara rationellt att låta polismyndigheterna ta över passhanteringen i sin helhet. Det bedömdes att det skulle leda till bättre och snabbare service för allmänheten. Passfrågorna ansågs dessutom ha ett nära samband med polismyndigheternas gränskontroll- och gränsövervakningsverksamhet (prop. 1977/78:156 s. 13–15).

Polismyndigheten är alltså passmyndighet inom landet. När det gäller utrikesrepresentationens roll är bilden något mer komplicerad. Utrikesrepresentationen består av bl.a. beskickningar (ambassader och legationer), karriärkonsulat (som ofta kallas generalkonsulat) och honorärkonsulat. Karriärkonsulaten leds av utsända tjänstemän och räknas liksom beskickningarna som utlandsmyndigheter. De skiljer sig därmed från honorärkonsulaten, som är underställda en utlandsmyndighet och leds av en person som är fast bosatt på den ort där honorärkonsulatet finns. En honorärkonsul är oavlönad.

Regeringskansliet beslutar i vilken utsträckning beskickningar och karriärkonsulat ska fullgöra uppgifter som passmyndigheter. Regeringskansliet får också besluta att honorärkonsulat i begränsad

utsträckning ska fullgöra uppgifter som passmyndighet (2 § tredje stycket passlagen och 28 a § passförordningen). Detta innebär att beskickningar och karriärkonsulat kan undantas från uppgiften att vara passmyndighet eller ges ett inskränkt uppdrag, t.ex. att bara utfärda provisoriska pass. I fråga om honorärkonsulat framgår det direkt av lagen att rollen som passmyndighet ska vara begränsad. När det i denna promemoria talas om konsulat som passmyndigheter är det alltså i praktiken karriärkonsulat som i första hand avses.

Vid sidan av passmyndigheterna får även Utrikesdepartementet utfärda pass, om det med hänsyn till allmän tjänst som sökanden har eller av någon annan anledning finns särskilda skäl (31 § passlagen). Formellt sett kan Utrikesdepartementet utfärda alla typer av pass. I praktiken handlar det dock om diplomat- och tjänstepass. Sådana pass får utfärdas endast av chefen för Utrikesdepartementet eller den han eller hon bemyndigar (17 § passförordningen). Organisatoriskt sett är Utrikesdepartementet ingen fristående myndighet, utan en del av Regeringskansliet. I författningar hänvisas det därför till ”Regeringskansliet (Utrikesdepartementet)”.

3.2.5 Vanliga pass och särskilda pass

Pass utfärdas som vanligt pass eller särskilt pass (3 § passlagen).

Kategorin särskilda pass innefattar provisoriska pass, extra pass, diplomatpass, tjänstepass och provisoriska resehandlingar enligt förordningen (1997:698) om Europeiska unionens provisoriska resehandling (3 § passlagen och 6 § passförordningen).

Vanligt pass

Varje svensk medborgare har rätt att efter ansökan få ett vanligt pass, om det inte finns något passhinder (4 § passlagen). Det betyder att en passmyndighet är skyldig att utfärda ett vanligt pass till en svensk medborgare, om förutsättningarna för det är uppfyllda. Ett vanligt pass gäller normalt för resor till alla länder och giltighetstiden är som huvudregel fem år eller, om sökanden ännu inte har fyllt tolv, tre år (3 § passlagen). I ett vanligt pass sparas passinnehavarens fingeravtryck och ansiktsbild i ett lagringsmedium (6 a § passlagen).

Provisoriskt pass

Ett provisoriskt pass kan utfärdas bl.a. om sökanden behöver ett pass omedelbart för en resa (11 § passförordningen). På en ansökan om ett provisoriskt pass ställs inte samma krav som på en ansökan om ett vanligt pass. Sökanden behöver bl.a. inte lämna sina fingeravtryck (12 a § passförordningen). Passets giltighetsområde ska begränsas till sökandens behov. Giltighetstiden ska begränsas till den tid som behövs för att sökanden ska kunna genomföra en viss resa, eller flera resor i omedelbar följd, och får inte överskrida sju månader (13 § passförordningen och 9 kap. 1 § PMFS 2019:3).

Extra pass

Ett extra pass får utfärdas för den som redan har ett vanligt pass men som för sitt arbete eller av något annat särskilt skäl behöver mer än ett giltigt pass (14 § passförordningen). Det kan handla exempelvis om att sökanden ska resa till länder mellan vilka det råder sådana politiska förhållanden som gör det mycket svårt att resa in i ett av länderna med ett vanligt pass som har använts för en resa till ett annat av länderna (10 kap. 1 § PMFS 2019:3).

Diplomat- och tjänstepass

Diplomat- och tjänstepass får som framgått utfärdas bara av chefen för Utrikesdepartementet eller den som han eller hon bemyndigar. Diplomattpass får utfärdas för medlemmar av kungafamiljen, statsråd och statssekreterare, tjänstemän inom utrikesförvaltningen m.fl. Tjänstepass får utfärdas för bl.a. riksdagsledamöter och personer som tjänstgör utomlands på uppdrag av bl.a. Försvarsmakten (2 och 3 §§ Regeringskansliets föreskrifter om diplomat- och tjänstepass).

Europeiska unionens provisoriska resehandling

Svenska passmyndigheter i utlandet får under vissa förutsättningar utfärda en provisorisk resehandling till en medborgare i ett annat EU-land. Villkoren är att det andra EU-landet saknar representation

på den aktuella orten, att sökandens pass har förkommit och att det andra EU-landet har gett sitt tillstånd till att resehandlingen utfärdas. Resehandlingen ska i princip gälla bara för sökandens hemresa till sitt medborgarskaps- eller bosättningsland (1 och 2 §§ förordningen om Europeiska unionens provisoriska resehandling).

3.2.6 Passhandläggningens olika delar

Hur en passansökan handläggs beror bl.a. på vilken typ av pass den gäller. Följande beskrivning gäller för en ansökan om vanligt pass som sökanden gör inom landet, hos Polismyndigheten.

Ärendet börjar med en passansökan

Den som vill ansöka om ett vanligt pass ska inställa sig personligen hos passmyndigheten (6 § passlagen). Ansökan ska göras på heder och samvete. Ansökan görs därmed under straffansvar. Sökanden är som huvudregel skyldig att låta passmyndigheten ta hans eller hennes fingeravtryck och en ansiktsbild i digitalt format. Sökanden ska vidare styrka sin identitet och sitt svenska medborgarskap.

Ansökan ska undertecknas av sökanden. Om han eller hon har ett giltigt pass sedan tidigare ska detta som huvudregel lämnas in i samband med ansökan om ett nytt pass (1 § passförordningen).

Om sökanden är under 18 år krävs vanligtvis att hans eller hennes vårdnadshavare lämnar sitt medgivande till att pass utfärdas. Finns det två vårdnadshavare krävs bådas samtycke. Medgivandet lämnas normalt på ett formulär (7 § 2 passlagen, 1 § passförordningen och 2 kap. 4 § PMFS 2019:3).

Sökanden ska betala en ansökningsavgift för att få sin ansökan prövad. Avgiften är för närvarande 350 kr (30 § passförordningen).

För vissa personer krävs passtillstånd

I vissa fall får pass inte utfärdas om sökanden inte har fått ett särskilt tillstånd till pass (passtillstånd). Detta framgår av 10 § passlagen.

Passtillstånd krävs till att börja med för den som avtjänar ett fängelsestraff, och inte är villkorligt frigiven, eller genomgår slutet

ungdomsvård. Om straffet eller vården är en månad eller kortare krävs dock inte passtillstånd. Passtillstånd krävs vidare för personer som står under övervakning efter en dom på skyddstillsyn eller efter villkorlig frigivning från fängelse (19 § passlagen).

Passtillstånd kan också krävas för personer som är intagna för psykiatrisk tvångsvård eller rättspsykiatrisk vård (20 § passlagen). I många fall gäller kravet på passtillstånd emellertid bara om chefsöverläkaren vid patientens sjukvårdsinrättning har anmält till Polismyndigheten att pass inte får utfärdas utan tillstånd.

Beslut om passtillstånd fattas, beroende på situation, av Kriminalvården, en övervakningsnämnd, Statens institutionsstyrelse eller Socialstyrelsen (21 och 22 §§ passlagen). Systemet med passtillstånd syftar bl.a. till att den vård som personen får inte ska äventyras genom att han eller hon får ett pass och åker utomlands.

Passmyndigheten prövar frågan om hinder

De allra flesta som ansöker om pass behöver inte ha passtillstånd. Det betyder emellertid inte att pass ska utfärdas utan vidare. Passmyndigheten ska alltid pröva om det finns hinder mot att pass utfärdas (3 § passförordningen). Om det finns ett sådant hinder ska ansökan som huvudregel avslås. Ett avslagsbeslut kan överklagas till allmän förvaltningsdomstol, dvs. förvaltningsrätt (27 § passlagen).

Vad som utgör hinder mot pass framgår av 7 § passlagen. En passansökan ska i regel avslås i följande fall:

1. De bestämmelser som gäller för en passansökan har inte iakttagits och sökanden har trots uppmaning inte rättat till bristen. Det kan handla om formella fel men också om att sökanden inte har styrkt sin identitet eller sitt svenska medborgarskap.
2. Ansökan gäller ett barn under 18 år och barnets vårdnadshavare har inte lämnat det medgivande som krävs. Om det finns synnerliga skäl får pass ändå utfärdas. Ett yttrande från socialnämnden kan då behöva hämtas in (3 § passförordningen).
3. Sökanden är anhållen, häktad eller underkastad övervakning, reseförbud eller anmälningsskyldighet enligt rättegångsbalken.
4. Sökanden är föremål för ett beslut om övervakningsåtgärder enligt 2 kap. 1 § lagen (2015:485) om erkännande och uppföljning

av beslut om övervakningsåtgärder inom Europeiska unionen och åklagare har inte lämnat medgivande till att pass utfärdas.

5. Sökanden är föremål för en uppföljningsförklaring som avser en övervakningsåtgärd enligt 3 kap. 3 § 3–5 ovan nämnda lag och åklagare har inte lämnat medgivande till att pass utfärdas.
6. Sökanden är efterlyst och ska omhändertas omedelbart vid anträffandet.
7. Sökanden har dömts till en frihetsberövande påföljd genom en dom som har fått laga kraft och har ännu inte börjat verkställa påföljden. Passhinder föreligger dock bara om det finns sannolika skäl att anta att sökanden vill undandra sig verkställigheten.
8. Sökanden avtjänar ett fängelsestraff, den sammanlagda tiden att avtjäna är minst ett år och sökanden har inte frigetts villkorligt.
9. Sökanden genomgår sluten ungdomsvård och den sammanlagda vårdtiden är minst ett år.
10. Sökanden genomgår rättspsykiatrisk vård med särskild utskrivningsprövning.
11. Sökanden är ålagd att lämna ifrån sig sitt pass enligt 2 kap. 12 § eller 6 kap. 6 § konkurslagen (1987:672) eller förbud att utfärda pass för sökanden har meddelats enligt samma bestämmelser.

Om det kommer fram att det kan finnas passhinder ska det göras en undersökning genom slagningar i misstankeregistret, belastningsregistret, personefterlysningsregistret, kriminalvårdsregistret och Schengens informationssystem (4 kap. 1 § PMFS 2019:3).

I praktiken är det Polismyndighetens datorsystem som signalerar att passhinder kan föreligga. När en ansökan registreras sker en automatisk kontroll mot de nämnda registren. Om personen förekommer i något av dem får passhandläggaren besked om detta. Handläggaren får veta vilket register det handlar om och kan också få ytterligare information från registret, för att kunna ta ställning till om det verkligen föreligger ett passhinder.

Det kan tilläggas att en passansökan ska avslås också om det inom de senaste fem åren före ansökan har utfärdats tre vanliga pass för sökanden och det inte finns särskilda skäl för att ändå bifalla ansökan (7 a § passlagen). Bestämmelsen ska motverka missbruk av pass.

Underrättelse till förundersökningsledare

Det faktum att någon är misstänkt för brott utgör inte i sig ett passhinder, så länge personen inte är t.ex. anhållen eller häktad.

I vissa fall ska dock passmyndigheten underrätta den som leder en förundersökning om att den som är skäligen misstänkt för brott har ansökt om ett pass (8 § passlagen). Det gäller om sökanden är misstänkt för ett brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader. I ett sådant fall får pass inte utfärdas innan en vecka har gått från det att underrättelsen lämnades. Pass får dock utfärdas tidigare om förundersökningsledaren medger det.

Syftet med bestämmelsen är att förundersökningsledaren ska få möjlighet att pröva frågan om att t.ex. anhålla den misstänkte, när det kommer fram att han eller hon har ansökt om pass. Om den misstänkte anhålls uppkommer ett passhinder och ansökan avslås.

Passet utfärdas och lämnas ut till sökanden

En svensk medborgare får som framgått vägras ett vanligt pass bara om det följer av passlagen (4 § passlagen). Om inget hinder kommer fram under handläggningen ska passet alltså utfärdas. Så snart som möjligt efter utfärdandet ska passet lämnas ut till sökanden personligen (21 § passförordningen). Sökanden måste alltså komma till passmyndigheten på nytt för att hämta ut sitt pass.

I vissa fall kan ett gällande pass återkallas

Sedan ett pass har utfärdats får det återkallas bara på de grunder som framgår av passlagen (4 § passlagen). Ett beslut om återkallelse kan överklagas till allmän förvaltningsdomstol. Återkallelsegrunderna framgår av 12 § passlagen och knyter delvis an till bestämmelserna om hinder mot pass. Ett pass ska återkallas i bl.a. följande fall:

1. Passinnehavaren har förlorat eller efter ansökan befriats från sitt svenska medborgarskap.
2. Passet avser ett barn under 18 år och barnets vårdnadshavare eller, om barnet vistas här i landet och står under vårdnad av båda

föräldrarna, en av dem begär att passet ska återkallas. Återkallelse ska dock inte ske om det finns synnerliga skäl mot det.

3. Passinnehavaren är efterlyst, ska omhändertas omedelbart vid anträffandet och uppehåller sig utomlands. Passet ska dock återkallas bara om det är motiverat av särskilda skäl.
4. Passinnehavaren har dömts till en frihetsberövande påföljd genom en dom som har fått laga kraft och har ännu inte börjat verkställa påföljden. Passet ska dock återkallas bara om det finns sannolika skäl att anta att passinnehavaren vill undandra sig verkställigheten.
5. Passinnehavaren avtjänar ett fängelsestraff, den sammanlagda tiden att avtjäna är minst ett år och passinnehavaren har inte frigetts villkorligt.
6. Passinnehavaren genomgår sluten ungdomsvård och den sammanlagda vårdtiden är minst ett år.
7. Passinnehavaren genomgår rättspsykiatrisk vård med särskild utskrivningsprövning.
8. Det förelåg hinder mot bifall till passansökan vid tiden för passets utfärdande och hindret består fortfarande.
9. Någon annan än den som passet är utställt för förfogar över det.

Om det finns grund för återkallelse kan passmyndigheten besluta om provisorisk återkallelse i högst sex månader (13 § passlagen).

Passmyndigheten kan, i stället för att återkalla passet, begränsa passets giltighetstid eller giltighetsområde. Det kräver att det finns särskilda skäl och att passinnehavaren begär det (14 § passlagen).

För den som avtjänar ett fängelsestraff, står under övervakning eller genomgår sluten ungdomsvård, psykiatrisk tvångsvård eller rättspsykiatrisk vård kan en övervakningsnämnd, Statens institutionsstyrelse eller Socialstyrelsen göra en framställning hos Polismyndigheten om att passet ska återkallas (24 § passlagen).

Om ett pass har återkallats, är passinnehavaren eller den som annars förfogar över passet skyldig att på begäran överlämna passet till passmyndigheten eller en annan myndighet (17 § passlagen). I avvaktan på ett slutligt beslut om återkallelse får passmyndigheten besluta att ett pass ska omhändertas (18 § passlagen).

3.2.7 Passkyldighet och passkontroll

Passlagen innehåller inte bara bestämmelser om rätten till pass och handläggningen av passansökningar och andra passfrågor. Som nämnts tidigare regleras även det s.k. passtvangen. I passlagen finns också vissa bestämmelser om passkontroller i samband med resor.

En svensk medborgare får som framgått inte resa ut ur landet utan att ha med sig ett giltigt pass (5 § första stycket passlagen). Det finns dock undantag från den huvudregeln. Ett sådant undantag är att passkyldigheten inte gäller vid resor till de EU-länder som har anslutit sig till Schengensamarbetet (5 § andra stycket 4 passlagen).

En svensk medborgare ska inte bara ha med sig ett giltigt pass vid utresa ur landet. Han eller hon ska även, som huvudregel, ha med sig ett giltigt pass vid inresa i Sverige från ett annat land (5 § tredje stycket passlagen). Detta krav gäller dock inte om det svenska medborgarskapet kan styrkas på annat sätt. Enligt 2 kap. 7 § första stycket regeringsformen får ingen svensk medborgare hindras från att resa in i landet. Förbudet är absolut och kan inte begränsas genom lag. Kravet på att föra med sig ett giltigt pass gäller inte vid inresa från något av de EU-länder som deltar i Schengensamarbetet.

Det är Polismyndigheten som ska övervaka att bestämmelserna i 5 § passlagen följs, dvs. att svenska medborgare som reser ut ur landet har med sig ett giltigt pass när detta krävs och att svenska medborgare som reser in i landet har med sig ett pass eller kan styrka sitt medborgarskap på annat sätt (5 a § passlagen). Det bör påpekas att 5 och 5 a §§ passlagen gäller endast för svenska medborgare. Kontrollen av utländska medborgare är reglerad i annan ordning.

Inom ramen för den kontroll som sker enligt passlagen är en svensk medborgare skyldig att lämna över sitt pass till en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Kustbevakningen, Tullverket eller Migrationsverket (5 a § andra stycket passlagen). Passinnehavaren ska också låta tjänstemannen ta hans eller hennes fingeravtryck och en bild i digitalt format av hans eller hennes ansikte för att kontrollera att dessa motsvarar de fingeravtryck och den ansiktsbild som finns sparade i passet.

3.3 Myndigheternas verksamhet i praktiken

3.3.1 En särskild uppgift för Polismyndigheten

Den nya Polismyndigheten bildades den 1 januari 2015 genom en sammanslagning av Rikspolisstyrelsen, Statens kriminaltekniska laboratorium och 21 fristående polismyndigheter. I dag består myndigheten av sju polisregioner och vissa nationella avdelningar. Polismyndigheten har för närvarande ca 30 000 medarbetare.

Till Polismyndighetens huvuduppgifter hör brottsförebyggande verksamhet, viss övervakning och brottsutredning. Därutöver har myndigheten vissa allmänna förvaltningsuppgifter med ett mer eller mindre nära samband med den egentliga polisverksamheten. Till dessa allmänna förvaltningsuppgifter hör passverksamheten.

De sju polisregionerna har ett helhetsansvar för verksamheten inom sina respektive geografiska områden. Ansvaret omfattar inte bara brottsbekämpningen utan också passverksamheten och övriga allmänna förvaltningsuppgifter. Inom varje polisregion finns ett antal passexpeditioner som handlägger frågor om pass och nationella identitetskort. Det går att ansöka om pass på valfri passexpedition. På passexpeditionerna arbetar både poliser och civilanställda. För närvarande arbetar ungefär 700 personer som passhandläggare.

Pass och nationella identitetskort är den största ärendegruppen inom Polismyndighetens allmänna förvaltningsverksamhet. Under 2017 hanterades drygt en och en halv miljon passansökningar. Antalet ansökningar var ungefär lika stort 2015 och 2016. Över 97 procent av ansökningarna avsåg vanligt pass. Resterande del avsåg provisoriskt pass och extra pass. Omkring 500 passansökningar avslogs under 2017, till följd av att sökanden inte hade styrkt sitt svenska medborgarskap, att sökanden inte hade kommit in med efterfrågade kompletteringar eller att det annars fanns passhinder.

3.3.2 Ambassaderna och konsulatet

Sverige har i dag drygt 100 ambassader, karriärkonsulat och andra utlandsmyndigheter. Därutöver finns det ca 340 honorärkonsulat.

En av ambassadernas och karriärkonsulatens huvuduppgifter är att verka för genomslag och förståelse för svenska ståndpunkter inom utrikespolitiken och andra politikområden. Ambassaderna och

karriärkonsulaten har därutöver flera andra uppgifter och till dem hör, som framgått, att fungera som passmyndigheter i utlandet.

En svensk medborgare som är bosatt i utlandet, eller som är på tillfälligt besök, kan alltså vända sig till vissa bestämda ambassader eller konsulat för att ansöka om nytt pass. Ansökningar om vanligt pass handläggs endast av ambassader och karriärkonsulat, inte av honorärkonsulat. Enligt Utrikesdepartementet går det att ansöka om vanligt pass vid ungefär 70 ambassader och karriärkonsulat. Ett trettiootal utlandsmyndigheter är alltså undantagna från uppgifter som passmyndighet. Att få ett vanligt pass hos en utlandsmyndighet tar längre tid än vad det gör hos Polismyndigheten, eftersom alla pass tillverkas i Sverige och därefter skickas till utlandsmyndigheten.

Till skillnad från vanliga pass tillverkas provisoriska pass på plats hos ambassaden eller konsulatet. Provisoriska pass utfärdas av alla ambassader och karriärkonsulat och även av vissa honorärkonsulat. Enligt Utrikesdepartementet finns det i dag ett hundratal honorärkonsulat som har fått bemyndiganden att utfärda provisoriska pass. Honorärkonsulat kan också bistå med att lämna ut pass som har utfärdats av någon annan passmyndighet.

Under 2017 utfärdades sammanlagt ungefär 27 000 vanliga pass och 5 000 provisoriska pass inom utrikesrepresentationen.

3.3.3 Protokollat inom Utrikesdepartementet

Diplomatpass och tjänstepass får som tidigare nämnts utfärdas bara av chefen för Utrikesdepartementet, dvs. utrikesministern, eller den som han eller hon bemyndigar. I praktiken har alla beslut i fråga om diplomat- och tjänstepass delegerats till chefen för Protokollat eller den som chefen för Protokollat bestämmer (7 § Regeringskansliets föreskrifter om diplomat- och tjänstepass). Protokollat är en enhet inom Utrikesdepartementet som ansvarar bl.a. för genomförande av statsbesök och kontakter med utländska ambassader m.m. Under 2017 utfärdades drygt 1 000 diplomatpass och ca 500 tjänstepass.

3.3.4 Passverksamheten är datoriserad

Polismyndigheten använder systemet RES

Polismyndigheten använder ett datoriserat ärendehanteringssystem för handläggning av passärenden. Systemet har tagits fram inom myndigheten och heter Resehandlingssystemet (RES). Alla ansökningar om pass handläggs i RES. Det finns dock en reservrutin som används när systemet inte fungerar. Sökanden fyller då i en blankett som registreras i RES i efterhand. Även återkallelser hanteras i RES.

RES används inte bara för handläggning av enskilda ärenden. Det fungerar också som ett register över utfärdade pass. I RES finns även ett register över vissa omständigheter som innebär att passtillstånd krävs för en person, bl.a. anmälningar från chefsöverläkare. RES är alltså ett stöd för både ärendehandläggning och registerföring.

Vid handläggningen av en passansökan hämtar RES automatiskt uppgifter från andra register. Folkbokföringsuppgifter hämtas från polisens person- och adressregister. Från de fotostationer som finns på passexpeditionerna hämtas sökandens ansiktsbild, fingeravtryck och namnteckning. RES hämtar också information om huruvida sökanden förekommer i belastningsregistret, misstankeregistret, personefterlysningsregistret eller kriminalvårdsregistret. Genom RES kan passhandläggaren också få ytterligare information från dessa register, om det visar sig att sökanden förekommer i dem.

Förutom att RES hämtar uppgifter från andra register lämnar datorsystemet också ut uppgifter om stulna eller förkomna pass till Schengens informationssystem (SIS) och till Interpol.

Övriga myndigheter använder systemet RES-UM

Ambassaderna, konsulaten och Utrikesdepartementet har tillgång till RES genom Resehandlingssystemet för utlandsmyndigheter (RES-UM). Detta system har tagits fram av Migrationsverket, som tillhandahåller flera av de datorprogram som utlandsmyndigheterna använder. RES-UM är ett ”arbetsfönster” som ger handläggaren en begränsad tillgång till RES. Genom RES-UM får handläggaren tillgång till information i RES och kan även spara uppgifter i RES. De ambassader och karriärkonsulat som utfärdar vanliga pass är utrustade med liknande fotostationer som Polismyndigheten.

Vid arbete i RES-UM hämtas sökandens folkbokföringsuppgifter och annan information från RES. Från RES hämtas även uppgifter om huruvida sökanden förekommer i belastningsregistret eller något av de andra register som Polismyndigheten har tillgång till. Handläggaren får dock inte veta vilket eller vilka register det är fråga om och har inte heller tillgång till registren. Om RES-UM visar att sökanden förekommer i ett register får frågan om passhinder därför utredas av Polismyndigheten, som gör de registerslagningar som behövs och därefter redovisar resultatet till utlandsmyndigheten.

Hur många personer har tillgång till datorsystemen?

Förutom passhandläggarna har även många andra anställda inom Polismyndigheten i olika utsträckning tillgång till datorsystemen. Utanför passmyndigheterna och Utrikesdepartementet har vissa anställda inom Migrationsverket tillgång till systemen, på grund av verkets arbete med RES-UM. Enligt uppgift från Polismyndigheten har systemen ca 30 000 användare allt som allt. Det finns ett tiotal behörighetsnivåer. De flesta användare har en begränsad behörighet som innebär att de kan se viss information men inte tillföra eller ändra uppgifter och inte heller utföra mer avancerade sökningar.

Tillgången till belastningsregistret och övriga register

Polismyndigheten är den myndighet som för belastningsregistret, misstankeregistret och personefterlysningsregistret. När frågor om passhinder undersöks gör myndigheten alltså slagningar i sina egna register. Från kriminalvårdsregistret får Polismyndigheten information genom Kriminalvården, som ansvarar för förandet av registret.

En passmyndighet i utlandet har en uttrycklig rätt att få uppgifter ur belastningsregistret och misstankeregistret, men inte genom direktåtkomst. Detta följer av förordningen (1999:1134) om belastningsregister och förordningen (1999:1135) om misstankeregister.

3.3.5 Handläggningen i RES och RES-UM

Tidigare i detta kapitel har passhandläggningen beskrivits utifrån bestämmelserna i passlagen. Det regelverket knyter inte an till något speciellt datorprogram eller annat handläggningsstöd. Den rättsliga översikten kompletteras i detta avsnitt med en praktisk beskrivning av handläggningen i RES och RES-UM. En utförligare beskrivning finns i promemorian Passdatalag (Ds 2015:44).

Ansökan registreras och vissa uppgifter hämtas

En passansökan görs elektroniskt och registreras i datorsystemet (RES eller RES-UM). Där registreras också att ansökningsavgiften har betalats. Datorsystemet hämtar automatiskt information om tidigare ansökningar, tidigare utfärdade pass och spärrade pass så att handläggaren har tillgång till de uppgifterna vid handläggningen. Som framgått hämtas även sökandens folkbokföringsuppgifter.

I samband med ansökan ska sökanden styrka sin identitet, vilket normalt görs genom en godkänd identitetshandling. Handläggaren noterar i datorsystemet på vilket sätt identiteten har styrkts.

Passhandläggaren ska vidare försäkra sig om att sökanden är svensk medborgare. Om sökanden ger in handlingar för att styrka sitt medborgarskap skannas dessa in och sparas i systemet. Samma sak gäller för andra handlingar som sökanden lämnar in i ärendet. Handläggaren kan också göra anteckningar i datorsystemet.

Sökanden fotograferas och lämnar fingeravtryck

I nästa steg tas ett digitalt fotografi av sökanden med hjälp av den fotostation som finns på passexpeditionen. Fotostationen är ansluten till datorsystemet. Även fingeravtryck och namnteckning tas upp med hjälp av fotostationen och registreras i datorsystemet.

Ansiktsbilden och fingeravtrycken genomgår en särskild teknisk behandling som säkerställer att de är användbara som underlag för biometrisk jämförelse. Biometri är en metod som kan användas för att identifiera en person med hjälp av hans eller hennes fysiologiska karaktärsdrag. Utifrån ett biometriskt underlag, t.ex. ett digitalt fotografi av ett ansikte eller ett fingeravtryck, går det att på teknisk

väg få fram mätdata, biometriska data, som kan användas som ett referensmaterial i syfte att säkert identifiera en viss person.

Ansiktsbilden, fingeravtrycken och namnteckningen sparas i ett lagringsmedium i passet. Ett lagringsmedium är en elektronisk minnesenhet (ett chip). Ansiktsbilden och namnteckningen sparas även i passregistret. Fingeravtrycken och de biometriska data som kan tas fram ur dessa och ur ansiktsbilden sparas inte i passregistret. De lagras en kortare tid i datorsystemet och förstörs därefter när passet har lämnats ut eller passansökan har återkallats eller avslagits. När ärendet är avslutat finns fingeravtrycken alltså bara i passet.

Datorsystemet ger signaler om eventuella passhinder

När en passansökan har registrerats i systemet sker som framgått en automatisk kontroll mot vissa register. Syftet är att handläggaren ska få besked om att det kan finnas ett passhinder. RES ger besked om sökanden förekommer i belastningsregistret, misstankeregistret, personefterlysningsregistret eller kriminalvårdsregistret. Genom RES kan handläggaren också få ytterligare information från dessa register, för utredningen av frågan om passhinder. I RES-UM anges bara att passansökan är ”under utredning”. Som nämnts är det Polismyndigheten som gör den utredning som behövs.

Datorsystemet visar inte bara om sökanden förekommer i de register som har nämnts ovan. Det ska också visa om sökanden behöver passtillstånd enligt 20 § 1 eller 3 passlagen. Den situation som avses är att sökanden är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård och att chefsöverläkaren vid sjukhuset har gjort en anmälan till Polismyndigheten om att pass inte får utfärdas utan passtillstånd. Det kan även vara fråga om att sökandens pass har återkallats efter en intagning för sådan vård, för att Socialstyrelsen i en framställning till Polismyndigheten bedömt att det med hänsyn till ändamålet med vården är olämpligt att han eller hon har pass.

Polismyndigheten för som framgått ett särskilt register över dessa omständigheter. Registret finns i RES och om sökanden förekommer i registret visar datorsystemet detta i samband med ansökan. Sådana anmälningar eller återkallelsebeslut som avses i 20 § 1 och 3 passlagen är i praktiken ovanliga och det förekommer att det aktuella registret inte innehåller några registreringar alls.

Beslut fattas och information överförs till passregistret

I normalfallet finns det ingen indikation om passhinder. Det betyder att passansökan ofta kan bifallas redan vid ansökningstillfället.

När frågan om passhinder måste utredas följer det ofta av passlagen eller passförordningen att ett yttrande ska hämtas in från någon annan myndighet, t.ex. Åklagarmyndigheten, Kriminalvården eller Socialstyrelsen. Yttrandet skannas in och sparas i systemet. Om pass inte kan utfärdas upprättas ett skriftligt beslut som sänds till sökanden. Beslutet skannas också in och sparas i datorsystemet.

Om ansökan bifalls skickas ett produktionsunderlag från RES till passtillverkaren, för närvarande AB Svenska Pass. Passet tillverkas och kan normalt hämtas ut hos passmyndigheten inom fem dagar. Om passet ska skickas till utlandet tar det längre tid.

När ett pass har lämnats ut förs uppgifterna i ärendet automatiskt över till passregistret. Alla uppgifter överförs dock inte. Sökandens fingeravtryck, och de biometriska data som kan tas fram ur dessa och ur ansiktusbilden, raderas som framgått. Eventuella uppgifter om att sökanden har förekommit i belastningsregistret, misstankeregistret, personefterlysningsregistret eller kriminalvårdsregistret förs inte heller över till passregistret. Att sökanden har förekommit i något av registren kan dock framgå av ett beslut eller av någon annan handling som har skannats in och sparats i ärendet.

Informationen i passregistret används på flera sätt

Passregistret används som framgått när en person ansöker om pass. Genom registret får passhandläggaren information om tidigare ansökningar, tidigare utfärdade pass och spärrade pass. Uppgifterna i passregistret används också på andra sätt inom passverksamheten.

Information i passregistret används även för andra ändamål. Polismyndigheten använder t.ex. fotografier ur registret för att identifiera personer vid större olyckor, vid fotokonfrontationer och som ett led i spaningsarbete. Fotografier lämnas också ut till andra myndigheter, t.ex. Säkerhetspolisen. Även information i enskilda passärenden kan emellanåt användas i andra sammanhang.

3.4 Personuppgifter och sekretess

3.4.1 Vad är en personuppgift?

Regelverket om personuppgiftsbehandling beskrivs i nästa kapitel. Det finns dock skäl att redan nu säga något om vilka personuppgifter som samlas in eller behandlas på andra sätt i passverksamheten.

Begreppet personuppgift har en vidsträckt innebörd. Enligt den rättsliga definitionen är en personuppgift varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Det betyder att all sorts information som direkt eller indirekt kan hänföras till en viss levande människa är en personuppgift.

Vissa personuppgifter betecknas som känsliga. Det gäller sådana personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening. Till samma kategori hör biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning. För känsliga personuppgifter gäller rättsligt sett ett särskilt skydd.

Även begreppet behandling av personuppgifter har en vidsträckt innebörd. Med behandling avses kort sagt alla åtgärder som vidtas i fråga om personuppgifter. Det kan handla om t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på något annat sätt, justering, sammanföring, begränsning, radering eller förstöring.

3.4.2 Personuppgifter i passärenden

Passmyndigheterna och Utrikesdepartementet behandlar ett flertal personuppgifter i sin verksamhet enligt passlagen. Uppgifterna avser i första hand den som har ansökt om pass eller har fått ett pass utfärdat. I begränsad utsträckning behandlas uppgifter även om andra personer, t.ex. passhandläggare och vårdnadshavare.

Vilka personuppgifter som behandlas i passverksamheten går inte att ange uttömmande. Det är inte möjligt att på förhand säga exakt vilken information som kan förekomma i handlingar som sökanden ger in eller vilka uppgifter som kan behövas för handläggningen.

Vissa personuppgifter behandlas dock regelmässigt, till följd av passlagens bestämmelser och de datorsystem som används. För att ringa in vilka uppgifter det handlar om är det lämpligt att skilja mellan handläggningen av enskilda ärenden och registerföringen.

När enskilda passärenden handläggs, med stöd av RES eller RES-UM, behandlas enligt Polismyndigheten följande uppgifter:

- sökandens personnummer
- sökandens fullständiga namn
- sökandens födelseort
- sökandens vårdnadshavare (om sökanden är under 18 år)
- sökandens kön
- sökandens medborgarskap
- sökandens telefonnummer (ej obligatorisk uppgift)
- sökandens mobiltelefonnummer (ej obligatorisk uppgift)
- sökandens e-postadress (ej obligatorisk uppgift)
- sökandens längd
- fotografi av sökandens ansikte
- sökandens fingeravtryck
- sökandens namnteckning
- personuppgifter i inskannade dokument (t.ex. personbevis)
- anteckningar av passhandläggare
- typ av pass
- ärendenummer
- passets giltighetstid
- passets giltighetsområde
- utfärdande myndighet
- passhandläggarens namn
- ansökningsdatum

- utfärdandedatum
- utlämningsställe
- avgift och betalningssätt
- legitimationssätt
- registrerande myndighet och handläggare
- passets status (t.ex. utlämnat eller utgången)
- liggetid hos myndigheten
- händelsehistorik.

Därutöver behandlas, som framgått tidigare, uppgifter om huruvida sökanden förekommer i misstankeregistret, belastningsregistret, personefterlysningsregistret eller kriminalvårdsregistret. Uppgifter som rör kravet på passtillstånd kan också förekomma.

3.4.3 Personuppgifter i Polismyndighetens register

Vid sidan av ärendehandläggningen behandlas personuppgifter i Polismyndighetens två register: passregistret och registret över sådana omständigheter som innebär att passtillstånd krävs enligt 20 § 1 och 3 passlagen. Båda dessa register förs med hjälp av RES.

Passregistret

Enligt Polismyndigheten finns följande uppgifter i registret:

- typ av pass
- passnummer
- innehavarens personnummer
- innehavarens kön
- innehavarens för- och efternamn
- innehavarens födelseort
- innehavarens längd

- utlämningsadress
- utfärdande myndighet
- namn på passhandläggaren som hanterade ansökan
- ansökningsdatum
- utfärdandedatum
- passets status (t.ex. utlämnat eller utgången)
- namn på passhandläggare som t.ex. makulerat ett pass
- passets giltighetstid
- passets giltighetsområde
- fotografi av innehavarens ansikte
- innehavarens namnteckning
- ärendenummer
- pagineringsnummer (i vissa äldre ärenden).

Enligt Polismyndigheten innehåller registret därutöver information om innehavarens passinnehav under de senaste ca 20 åren.

Registret över vissa omständigheter som innebär att passtillstånd krävs

Registret avser personer som är intagna för psykiatrisk tvångsvård eller rättspsykiatrisk vård och som behöver passtillstånd till följd av en anmälan från en chefsöverläkare eller för att ett tidigare utfärdat pass har återkallats efter framställning från Socialstyrelsen. Enligt Polismyndigheten kan detta register innehålla följande uppgifter:

- patientens namn
- patientens personnummer
- passhandläggares anteckningar
- registreringsdatum
- uppgifter om vem som har registrerat informationen.

Handlingar i ärenden om passstillstånd skannas enligt Polismyndigheten inte in, utan diarieförs i myndighetens allmänna diarium och förvaras i en akt.

3.4.4 Sekretess i passverksamheten

De uppgifter som förekommer i passverksamheten kan i de flesta fall betraktas som harmlösa (jfr propositionen Ökad säkerhet i pass m.m., prop. 2004/05:119 s. 44 f.). Detta gäller dock inte utan undantag och det finns därför vissa bestämmelser om sekretess.

Bestämmelser om sekretess för uppgifter i passregistret finns i 22 kap. 1 § offentlighets- och sekretesslagen (2009:400) jämförd med 6 § offentlighets- och sekretessförordningen (2009:641).

Av dessa bestämmelser framgår att sekretess gäller för

- uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och
- uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

När det gäller fotografierna i passregistret innebär bestämmelserna att det råder en presumtion för sekretess. En begäran om att få ut ett fotografi bedöms därför ingående och den som begär ut fotografiet måste vanligtvis redogöra både för sin identitet och för syftet med sin begäran (jfr propositionen Några frågor om sekretess, m.m., prop. 2003/04:93 s. 39 f.). För övriga uppgifter som förekommer i passregistret råder däremot en stark presumtion för offentlighet.

Den beskrivna sekretessen gäller i sådan verksamhet som avser passregistret. För sådana uppgifter i passärenden som inte är avsedda att registreras i passregistret regleras sekretessen i 35 kap. 22 § offentlighets- och sekretesslagen. Där anges det att sekretess gäller i ett ärende enligt passlagen för uppgift om en enskilds personliga förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Sekretessen gäller inte för uppgifter i ett beslut. Bestämmelsen är utformad med ett rakt skaderekvisit, dvs. en presumtion för offentlighet. I förarbetena (prop. 2004/05:119 s. 55) anges att uppgifter som normalt sett är

harmlösa därmed i regel kan lämnas ut utan någon närmare skadebedömning i det enskilda fallet. Typiskt sett känsliga uppgifter omfattas däremot normalt av sekretess. Som exempel nämns i förarbetena uppgifter i ärenden om passtillstånd för den som är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård.

De biometriska data som tas fram vid en passansökan anses inte utgöra en allmän handling utan en mellanprodukt till det färdiga passet. Någon bestämmelse om sekretess för dessa uppgifter har därför inte varit aktuell att införa (prop. 2004/05:119 s. 45 f.).

4 Regelverket om dataskydd

4.1 En översikt över regelverket

I det här kapitlet beskrivs regelverket om dataskydd eller, med andra ord, de bestämmelser som gäller för behandling av personuppgifter.

Kapitlet inleds med en genomgång av det grundläggande skyddet för den personliga integriteten. Rätten till respekt för privatlivet är en viktig del av flera konventioner om mänskliga rättigheter och registrering av personuppgifter kan i vissa fall beröra den rätten. Flera internationella organisationer, som Europarådet, har därför arbetat fram konventioner om skydd vid databehandling. Även den svenska grundlagen skyddar enskildas personliga integritet.

För svensk del fanns närmare bestämmelser om behandling av personuppgifter tidigare i personuppgiftslagen (1998:204). Lagen har dock upphävts till följd av den dataskyddsreform som har ägt rum inom EU. Efter reformen finns det två huvudsakliga regelverk om personuppgiftsbehandling, som båda beskrivs i detta kapitel.

Den generella regleringen av personuppgiftsbehandling inom EU finns i den s.k. dataskyddsförordningen, som tillämpas i unionen sedan den 25 maj 2018. Förordningen är direkt tillämplig men kompletteras i flera avseenden av svenska lagar och förordningar.

När bl.a. polis, åklagare och allmänna domstolar behandlar personuppgifter inom ramen för brottsbekämpning, lagföring och straffverkställighet gäller i stället ett nytt EU-direktiv, som i Sverige i huvudsak har genomförts genom brottsdatalagen (2018:1177).

Sista delen av kapitlet handlar om personuppgiftsbehandlingen i passverksamheten. Det konstateras att personuppgiftslagen tidigare gällde för denna behandling och att det finns vissa bestämmelser i passlagen och passförordningen som kan anses ta sikte på just behandling av personuppgifter. Frågan om vilket regelverk som

numera gäller för passverksamheten, dataskyddsförordningen eller brottsdatalagen eller möjligen båda två, behandlas i nästa kapitel.

4.2 Det grundläggande integritetsskyddet

4.2.1 Överenskommelser inom FN och OECD

FN och de mänskliga rättigheterna

Den allmänna förklaringen om de mänskliga rättigheterna antogs av Förenta nationerna (FN) 1948. Förklaringen är inte formellt bindande men ses som ett uttryck för sedvanerättsliga regler.

Skyddet för den personliga integriteten, eller den privata sfären, behandlas i artikel 12. Där anges att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.

Vid utövandet av sina rättigheter och friheter enligt den allmänna förklaringen får en person, enligt artikel 29 i förklaringen, endast underkastas sådana inskränkningar som har fastställts i lag och bara i syfte att trygga tillbörlig hänsyn till och respekt för andras rättigheter och friheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

Inom FN har det också utarbetats en internationell konvention om medborgerliga och politiska rättigheter. Sverige har anslutit sig till konventionen, som trädde i kraft 1976. I konventionens artikel 17 upprepas det som sägs i artikel 12 i den allmänna förklaringen.

Slutligen antog FN:s generalförsamling under 1990 riktlinjer om datoriserade register med personuppgifter. I riktlinjerna finns vissa grundläggande principer som medlemsstaterna ska ta hänsyn till vid lagstiftning om sådana register. Det framgår bl.a. att det bör finnas särskilt angivna och legitima ändamål för datoriserade register.

Riktlinjer från OECD

Organisationen för ekonomiskt samarbete och utveckling (OECD) antog 1980 riktlinjer för skyddet av den personliga integriteten och gränsöverskridande flöden av personuppgifter. Riktlinjerna gäller för både privat och offentlig verksamhet och ska uppfattas som

minimiregler. Det framgår bl.a. att personuppgifter i regel inte ska användas för andra syften än de som uppgifterna samlades in för. Riktlinjerna antogs tillsammans med en rekommendation till medlemsstaternas regeringar om att beakta riktlinjerna i nationell lagstiftning. Sverige har åtagit sig att följa riktlinjerna.

4.2.2 Europarådets konventioner och EU-stadgan

Europarådet är en mellanstatlig organisation, skild från EU, som bildades 1949 och som arbetar för mänskliga rättigheter, demokrati och rättsstatens principer (eng. rule of law). Inom ramen för Europarådet har flera konventioner som rör integritetsskydd utarbetats.

Europakonventionen om mänskliga rättigheter

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som lag i Sverige sedan den 1 januari 1995. Lagar och andra föreskrifter får enligt 2 kap. 19 § regeringsformen inte meddelas i strid med Sveriges åtaganden på grund av konventionen.

Skyddet för den personliga integriteten behandlas i artikel 8. Där anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentliga myndigheter får inte inskränka 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.

Registrering av personuppgifter kan i vissa fall beröra rätten till respekt för privatlivet enligt artikel 8 (jfr Danelius, Mänskliga rättigheter i europeisk praxis, femte upplagan, s. 386–391).

Europarådets dataskyddskonvention

Vid sidan av Europakonventionen har Europarådet tagit fram en konvention om skydd för enskilda vid automatisk databehandling av

personuppgifter (dataskyddskonventionen). Sverige har anslutit sig till konventionen, som trädde i kraft den 1 oktober 1985.

Dataskyddskonventionen innehåller grundläggande principer om dataskydd som konventionsstaterna ska beakta i sin nationella lagstiftning. Syftet är att säkerställa rätten till personlig integritet i samband med automatiserad behandling av personuppgifter. Konventionen gäller för både privat och offentlig verksamhet.

Av konventionen framgår bl.a. att personuppgifter ska inhämtas och behandlas på ett korrekt sätt och vara relevanta med hänsyn till ändamålet. Vissa kategorier av personuppgifter får inte behandlas genom automatiserad databehandling om inte den nationella lagstiftningen ger ett ändamålsenligt skydd. Det gäller bl.a. sådana personuppgifter som avslöjar ras eller politiska åsikter eller som rör hälsa. Det gäller också uppgifter om att någon har dömts för brott.

I syfte att modernisera konventionen har en översyn pågått inom Europarådet. Förhandlingarna resulterade i maj 2018 i att ett ändringsprotokoll antogs. Sverige tillhörde de första konventionsstaterna att underteckna protokollet. Processen för att ändringsprotokollet ska träda i kraft har därmed inletts.

Europarådet har även antagit ett antal rekommendationer på dataskyddsområdet. Rekommendationerna är dock inte bindande.

EU-stadgan om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna (stadgan) antogs 2000 och är sedan 2009 rättsligt bindande för EU-institutionerna och medlemsstaterna när de tillämpar unionsrätt.

Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer.

Av artikel 8 i stadgan framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

4.2.3 Regeringsformens integritetsskydd

Även den svenska grundlagen ger den enskilde ett grundläggande skydd för den personliga integriteten. Av 1 kap. 2 § regeringsformen framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet. Det allmänna ska enligt samma paragraf värna den enskildes privatliv och familjeliv.

För att ytterligare stärka skyddet för den personliga integriteten infördes den 1 januari 2011 en ny bestämmelse i 2 kap. 6 § andra stycket regeringsformen. I den anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Detta skydd för den personliga integriteten får enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen som en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

4.3 Reglerna om personuppgiftsbehandling

4.3.1 Tidigare gällde personuppgiftslagen

För svensk del har de närmare bestämmelserna om behandling av personuppgifter under ganska lång tid grundat sig på unionsrätt.

De allmänna reglerna om behandling av personuppgifter inom EU fanns före dataskyddsreformen i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (1995 års dataskyddsdirektiv).

Direktivet gällde inte för personuppgiftsbehandling på områden utanför unionsrätten, t.ex. statens verksamhet på straffrättens område. Delar av den behandlingen omfattades i stället av rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet).

I svensk rätt genomfördes 1995 års dataskyddsdirektiv framför allt genom personuppgiftslagen, medan dataskyddsrambeslutet genomfördes i huvudsak genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

Personuppgiftslagen trädde i kraft den 24 oktober 1998 och hade ett vidsträckt tillämpningsområde. Sverige valde att göra lagen tillämplig även utanför unionsrättens område och den gällde för både myndigheter och enskilda. Personuppgiftslagen innehöll ett antal grundläggande krav på behandlingen av personuppgifter, t.ex. att personuppgifter fick samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål samt att uppgifterna skulle vara adekvata och relevanta i förhållande till dessa ändamål. Lagen innehöll också bestämmelser om när behandling av personuppgifter alls var tillåten, när behandling av känsliga personuppgifter var tillåten, vilken information som skulle lämnas till registrerade, vilka säkerhetskrav som gällde vid behandlingen, när personuppgifter fick föras över till länder utanför EU, när registrerade hade rätt till skadestånd osv.

Personuppgiftslagen var subsidiär, vilket innebar att den inte skulle tillämpas om det fanns avvikande bestämmelser i en annan lag eller förordning. Detta öppnade upp för ett system med avvikande eller mer detaljerade bestämmelser i sektorsspecifika författningar. Sådana författningar, s.k. registerförfattningar, finns fortfarande och reglerar ofta hur vissa myndigheter får behandla personuppgifter. Som exempel kan domstolsdatalagen (2015:728) nämnas.

Personuppgiftslagen och de olika registerförfattningarna bildade tillsammans det regelverk som gällde före dataskyddsreformen.

4.3.2 Dataskyddsreformen innebär nya regler

Under 2012 föreslog Europeiska kommissionen en genomgripande reform av unionens bestämmelser om skydd för personuppgifter.

Förslaget omfattade till att börja med en EU-förordning med allmänna regler om skydd för personuppgifter, som skulle ersätta 1995 års dataskyddsdirektiv. Förslaget omfattade vidare ett nytt direktiv med regler om skydd för personuppgifter i samband med bl.a. brottsbekämpning, lagföring och straffverkställighet. Detta direktiv skulle ersätta dataskyddsrambeslutet från 2008.

En politisk överenskommelse om reformen nåddes i slutet av 2015 och i april 2016 kunde två nya rättsakter antas:

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
- Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

Den allmänna dataskyddsförordningen kallas i vardagligt tal ofta för GDPR (eng. General Data Protection Regulation). Här används i stället benämningen dataskyddsförordningen eller förordningen. Direktivet omnämns som 2016 års dataskyddsdirektiv.

Till följd av reformen har personuppgiftslagen upphävts. Det har också skett ett omfattande arbete med att anpassa de svenska registerförfattningarna till de nya rättsakterna. De nya reglerna på förordningens respektive direktivets område beskrivs nedan.

4.3.3 Dataskyddsförordningens regelverk

Dataskyddsförordningen liknar delvis ett direktiv

Dataskyddsförordningen tillämpas från och med den 25 maj 2018. Sedan dess utgör förordningen den generella och grundläggande regleringen av personuppgiftsbehandling inom unionen.

Dataskyddsförordningen är, i likhet med andra EU-förordningar, till alla delar bindande och direkt tillämplig i varje medlemsstat. Det betyder att bestämmelserna i förordningen ska tillämpas direkt av enskilda och myndigheter, på samma sätt som lagar och andra nationella föreskrifter. Detta skiljer en EU-förordning från ett EU-direktiv, som i princip ska genomföras genom nationell lagstiftning.

Trots att dataskyddsförordningen är direkt tillämplig innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. Förordningen

har därmed i vissa delar en direktivliknande karaktär och kan, när det anges, fyllas ut eller preciseras genom nationella bestämmelser.

Dataskyddsförordningen ska ge ett enhetligt skydd

Ett huvudsakligt syfte med dataskyddsförordningen är, enligt skälen till förordningen, att säkerställa en enhetlig skyddsnivå över hela unionen och att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden. För att nå det målet behövs det enligt skälen en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer och som ger fysiska personer i alla medlemsstater samma rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar. På så sätt blir övervakningen av behandlingen av personuppgifter enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt.

Tillämpningsområdet är begränsat i några avseenden

Dataskyddsförordningen ska som utgångspunkt tillämpas på all behandling av personuppgifter som företas helt eller delvis på automatisk väg, t.ex. med hjälp av datorer. Den ska också tillämpas på manuell behandling av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1 i dataskyddsförordningen).

Tillämpningsområdet är ändå begränsat i några avseenden. Till att börja med undantas behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken (artikel 2.2 a och b). Som utvecklas längre fram har Sverige emellertid valt att göra förordningen tillämplig även utanför unionsrättens område.

Ett annat undantag är att dataskyddsförordningen inte ska tillämpas på behandling av personuppgifter som vissa myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. I detta ingår även sådan behandling som utförs i syfte att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.2 d). Sådan

behandling faller utanför förordningens tillämpningsområde och regleras i stället exklusivt av 2016 års dataskyddsdirektiv.

Många av de materiella bestämmelserna går att känna igen

När det gäller struktur och innehåll baseras dataskyddsförordningen till stor del på 1995 års dataskyddsdirektiv. Många bestämmelser går därför att känna igen från personuppgiftslagen, som genomförde det direktivet. Förordningen innebär emellertid vissa förändringar i sak. Bland annat har den registrerades rättigheter förstärkts på vissa sätt och ett system med administrativa sanktionsavgifter har införts.

Det kan finnas skäl att redan här översiktligt redovisa innehållet i förordningen, för att ge överblick. Vissa bestämmelser behandlas närmare i anslutning till bedömningar och förslag längre fram.

Kapitel I i förordningen innehåller allmänna bestämmelser om förordningens syfte och förordningens materiella och territoriella tillämpningsområde. I kapitlet definieras också vissa begrepp, som t.ex. personuppgifter, behandling och personuppgiftsansvarig.

Kapitel II innehåller vissa grundläggande principer som ska gälla vid behandling av personuppgifter. Det anges bl.a. att uppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Av kapitlet framgår också att personuppgifter får behandlas bara om vissa villkor är uppfyllda, dvs. om det finns en rättslig grund för behandlingen. Kapitlet innehåller också regler om behandlingen av särskilda kategorier av personuppgifter (känsliga personuppgifter) och uppgifter om fällande domar i brottmål.

Kapitel III handlar om den registrerades rättigheter, bl.a. rätten att få information om behandlingen, rätten att få tillgång till de personuppgifter som behandlas och rätten till rättelse och radering.

Kapitel IV behandlar den personuppgiftsansvariges skyldigheter och vad som gäller om ett personuppgiftsbiträde anlitas. Här finns också bestämmelser om säkerhet vid personuppgiftsbehandling.

Kapitel V handlar om överföring av personuppgifter till länder utanför EU eller till internationella organisationer.

Kapitel VI reglerar tillsynen över bestämmelserna i förordningen. Kapitlet efter gäller samarbetet mellan tillsynsmyndigheterna.

Kapitel VIII handlar om rättsmedel, t.ex. överklagande av vissa beslut, samt ersättning vid överträdelser av förordningen. Även det nya systemet med administrativa sanktionsavgifter behandlas.

Kapitel IX handlar om särskilda behandlingssituationer. I två avslutande kapitel finns bestämmelser av formell karaktär, bl.a. om ikraftträdande och om upphävande av 1995 års dataskyddsdirektiv.

Det finns kompletterande svenska bestämmelser

Dataskyddsförordningen innehåller som framgått ett stort antal bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser. Kompletterande bestämmelser av generellt slag finns för svensk del i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Enligt dataskyddslagen ska dataskyddsförordningen för svensk del tillämpas även vid personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, samt i sådan verksamhet som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken (2 kap. 1 § dataskyddslagen). Det betyder att förordningens bestämmelser gäller som svensk rätt även vid behandling av personuppgifter som utförs i verksamheter som egentligen är undantagna från förordningens tillämpningsområde.

Dataskyddslagen innehåller i övrigt bestämmelser som preciserar och kompletterar dataskyddsförordningen i fråga om bl.a. rättslig grund för behandling av personuppgifter samt behandling av känsliga personuppgifter. Eftersom lagen är kompletterande kan den inte tillämpas fristående utan bara tillsammans med förordningen.

Dataskyddslagen trädde i kraft den 25 maj 2018, dvs. samma dag som dataskyddsförordningen började tillämpas. Samtidigt upphörde personuppgiftslagen att gälla. Dataskyddslagen kompletteras av förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Av den förordningen framgår bl.a. att det är Datainspektionen som ansvarar för tillsynen på området.

Dataskyddslagen innehåller sådana kompletterande föreskrifter till dataskyddsförordningen som gäller på ett generellt plan. Lagen är subsidiär på så sätt att avvikande bestämmelser i andra lagar eller förordningar har företräde framför lagen. Närmare bestämmelser om personuppgiftsbehandling i vissa verksamheter finns alltså i

särskilda registerförfattningar och dessa har alltså företrädde framför de allmänna reglerna i dataskyddslagen. Registerförfattningarna har dock setts över och anpassats till dataskyddsförordningen.

Sammanfattningsvis kan sägas att det generella regelverket för personuppgiftsbehandling numera finns i dataskyddsförordningen medan svensk rätt – dataskyddslagen och registerförfattningarna – innehåller kompletterande bestämmelser till förordningen.

4.3.4 Brottsdatalagens regelverk

Brottsdatalagen genomför direktivet i svensk rätt

Vid sidan av dataskyddsförordningen består dataskyddsreformen av 2016 års dataskyddsdirektiv, som avser skydd för personuppgifter vid bl.a. brottsbekämpning, lagföring och straffverkställighet. Detta har i svensk rätt i huvudsak genomförts genom en ny ramlag, brottsdatalagen, som trädde i kraft den 1 augusti 2018. Samtidigt upphävdes den lag som hade genomfört dataskyddsrambeslutet.

Brottsdatalagen har ett avgränsat tillämpningsområde

Brottsdatalagen gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet (1 kap. 2 § brottsdatalagen).

Med behörig myndighet menas i första hand en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte (1 kap. 6 § brottsdatalagen). Ett exempel på en sådan myndighet är Polismyndigheten. För att vara behörig i brottsdatalagens mening krävs dock att Polismyndigheten behandlar personuppgifter för vissa syften, som att utreda brott.

För att brottsdatalagen ska vara tillämplig krävs vidare att behandlingen av personuppgifterna är helt eller delvis automatiserad

eller, om behandlingen är manuell, att personuppgifterna ingår i eller är avsedda att ingå i en viss sorts register (1 kap. 3 § brottsdatalagen).

Bestämmelserna liknar dem i dataskyddsförordningen

Syftet med brottsdatalagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt (1 kap. 1 § brottsdatalagen).

I sak påminner bestämmelserna i brottsdatalagen om dem i dataskyddsförordningen, även om det finns skillnader. I lagen finns bestämmelser om bl.a. grundläggande krav på behandlingen, längsta tid som personuppgifter får behandlas, personuppgiftsansvarigas skyldigheter, enskildas rättigheter, tillsyn och sanktionsavgifter.

Det finns kompletterande bestämmelser till lagen

Brottsdatalagen innehåller generella bestämmelser som gäller för behöriga myndigheter när de behandlar personuppgifter för de syften som anges i lagen. Vissa kompletterande bestämmelser till brottsdatalagen finns i brottsdataförordningen (2018:1202).

Brottsdatalagen är subsidiär i förhållande till andra lagar och förordningar. Det möjliggör registerförfattningar med avvikande bestämmelser även på brottsdatalagens område. Sådana lagar och förordningar finns för bl.a. polis- och åklagarmyndigheterna. Även dessa författningar har setts över och anpassats, så att de ska vara förenliga med brottsdatalagen och 2016 års dataskyddsdirektiv.

4.4 Särskilda regler för passverksamheten

4.4.1 Ingen särskild registerförfattning

Före dataskyddsreformen gällde personuppgiftslagen för den behandling av personuppgifter som förekom i passverksamheten. Någon särskild registerförfattning fanns inte och finns fortfarande inte. Det finns däremot vissa regler i passlagen och passförordningen som kan anses ta sikte på just behandlingen av personuppgifter.

4.4.2 Bestämmelser om Polismyndighetens register

I 23 § passförordningen anges att Polismyndigheten ska föra ett passregister och ett register över omständigheter som avses i 20 § 1 och 3 passlagen. Polismyndigheten ska alltså föra två olika register.

Passregistret är, som framgått i förra kapitlet, ett register över utfärdade pass. Enligt 23 § passförordningen ska Polismyndigheten på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen, Ekobrottsmyndigheten, en svensk ambassad, ett svenskt lönat konsulat, Försvarsmakten, Kustbevakningen, Tullverket, Skatteverket och Kronofogdemyndigheten. I övrigt finns det inte några särskilda bestämmelser om passregistret.

Det andra registret avser vissa omständigheter som innebär att passtillstånd kan behövas. Den situation som avses är till att börja med att sökanden är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård och att chefsöverläkaren vid sjukhuset har anmält till Polismyndigheten att pass inte får utfärdas utan tillstånd. Det är vidare fråga om att sökandens pass har återkallats efter en intagning för sådan vård, för att Socialstyrelsen i en framställning till Polismyndigheten har bedömt att det med hänsyn till ändamålet med vården är olämpligt att han eller hon har pass. Inte heller detta register är närmare reglerat i passlagen eller passförordningen.

4.4.3 Bestämmelser om biometriska data

Vid en passansökan är sökanden skyldig att låta passmyndigheten ta hans eller hennes fingeravtryck och en ansiktsbild i digitalt format.

Fingeravtrycken och ansiktsbilden ska enligt 6 a § passlagen sparas i ett lagringsmedium i passet. Detta är, som beskrivits tidigare, ett chip. Av 22 a § passförordningen framgår att passinnehavaren har rätt att kontrollera den information som har sparats i lagringsmediet.

Av 6 a § passlagen framgår att fingeravtrycken och de biometriska data som tas fram ur dessa och ur ansiktsbilden omedelbart ska förstöras när passet har lämnats ut eller när passansökan har återkallats eller avslagits. Fingeravtrycken och ansiktsbilden samt de biometriska data som kan tas fram ur dessa får enligt 6 b § passlagen inte användas vid sökning med hjälp av automatiserad behandling.

Bestämmelserna innebär bl.a. att det inte finns något hinder mot att spara ansiktsbilden i passregistret, medan fingeravtrycken inte

får sparas någon annanstans än i passet. Det finns därmed ingen möjlighet att bygga upp ett separat fingeravtrycksregister med hjälp av de fingeravtryck som lämnas i samband med passansökningar (jfr propositionen Fingeravtryck i pass, prop. 2008/09:132 s. 16). Det är inte heller tillåtet att använda ansiktsbilden, fingeravtrycken eller de biometriska data som kan tas fram ur dessa vid sökning med hjälp av automatiserad behandling t.ex. för identifiering av en okänd person (jfr prop. 2008/09:132 s. 16 och prop. 2004/05:119 s. 25).

Slutligen bör bestämmelserna i 5 a § passlagen nämnas, även om de riktar sig till pass- och gränskontrollanter och inte till de myndigheter som utfärdar pass. Av paragrafen framgår att den som ska ha med sig ett svenskt pass vid utresa ur eller inresa i Sverige är skyldig att på begäran lämna över passet till en kontrollant och dessutom låta kontrollanten ta hans eller hennes fingeravtryck och ansiktsbild, för kontroll av att dessa motsvarar de fingeravtryck och den ansiktsbild som finns sparade i passet. När kontrollen har genomförts ska fingeravtrycken och ansiktsbilden samt de biometriska data som har tagits fram omedelbart förstöras. Syftet med kontrollen är alltså bara att se om det är rätt person som innehar passet, inte att skapa ett fotoregister eller ett register med biometriska data över dem som passerar gränskontrollen. Det får således inte ske någon lagring av kontrollunderlaget.

5 En passdatalag bör införas

5.1 Frågor som behöver övervägas

I promemorian Passdatalag (Ds 2015:44) föreslogs en särskild lag om passmyndigheternas och Utrikesdepartementets behandling av personuppgifter i passverksamheten. Enligt förslaget skulle den ha namnet passdatalag. Lagen skulle gälla utöver personuppgiftslagen och innehålla bestämmelser anpassade för just passverksamheten.

Frågan är om det fortfarande, sedan dataskyddsreformen har genomförts och personuppgiftslagen har upphävts, bör införas en särskild lag om personuppgiftsbehandlingen i passverksamheten. För att ta ställning till det behöver ett antal delfrågor analyseras.

Till att börja med är det nödvändigt att bedöma vilket av de två nya regelverken för personuppgiftsbehandling som är tillämpligt, brottsdatalagen eller dataskyddsförordningen. Vilken anknytning har den personuppgiftsbehandling som sker i passverksamheten till exempelvis brottsbekämpning, lagföring och straffverkställighet?

När det har konstaterats vilket av regelverken som gäller måste det, i vart fall om dataskyddsförordningen är tillämplig, bedömas om det finns utrymme för nationella bestämmelser om behandlingen av personuppgifter i passverksamheten. Det måste också bedömas om sådana regler behövs. Om närmare bestämmelser på nationell nivå kan och bör införas är frågan slutligen om dessa ska meddelas av riksdagen genom lag eller av regeringen genom förordning. Frågan om normgivningsnivå ska bedömas utifrån regeringsformen.

Vid genomgången av dessa frågor, i fortsättningen av kapitlet, redovisas bedömningarna och förslagen i den tidigare promemorian tillsammans med remissinstansernas synpunkter på dem. Eftersom promemorian upprättades före dataskyddsreformen innehåller den emellertid inte bedömningar och förslag i alla delar.

5.2 Brottsdatalagen är inte tillämplig

Bedömning: Brottsdatalagen gäller inte när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter inom ramen för passverksamheten, dvs. verksamhet enligt passlagen.

Den tidigare promemorian innehåller ingen bedömning i frågan. Remissinstanserna yttrar sig inte i frågan.

Skälen för bedömningen

Brottsdatalagens tillämpningsområde

Brottsdatalagen gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som behöriga myndigheter utför i syfte att upprätthålla allmän ordning och säkerhet (2 kap. 1 § brottsdatalagen).

Med behörig myndighet avses i första hand en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte (1 kap. 6 § brottsdatalagen).

Bestämmelserna innebär att lagens tillämpningsområde är knutet både till vilket syfte en viss behandling av personuppgifter har och till vilken myndighet som utför behandlingen. För att lagen ska gälla krävs dels att behandlingen har ett sådant syfte som anges i lagen, t.ex. brottsbekämpning, dels att myndigheten i fråga är behörig.

Vilka myndigheter som är behöriga framgår inte direkt av lagen. Det avgörande är om myndigheten har uppgifter som faller inom området för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten och Kriminalvården m.fl. är alla myndigheter som kan vara behöriga, men bara när de behandlar personuppgifter för sådana syften som anges i lagen. Vid behandling för andra syften gäller i regel dataskyddsförordningen.

Regleringen innebär att brottsdatalagen gäller t.ex. när Polismyndigheten behandlar personuppgifter inom underrättelseverksamhet,

annan brottsförebyggande verksamhet eller förundersökning. Lagen gäller också när Polismyndigheten behandlar personuppgifter för ordningshållande syften vid sidan av den traditionella brottsbekämpningen, t.ex. i samband med avlägsnanden av personer m.m.

Tillämpningsområdet och gränsen mot dataskyddsförordningen behandlas närmare i lagens förarbeten (betänkandet Brotttsdatalag, SOU 2017:29, och propositionen Brotttsdatalag, prop. 2017/18:232).

Passverksamheten faller utanför brotttsdatalagens tillämpningsområde

Frågan om brotttsdatalagen gäller när personuppgifter behandlas i passverksamheten tar sikte främst på Polismyndigheten. De övriga myndigheter som handlägger passärenden – vissa ambassader och konsulat samt Utrikesdepartementet – har inte brottsbekämpande uppdrag eller andra uppgifter av det slag som gör lagen tillämplig. Deras behandling av personuppgifter faller således utanför lagens tillämpningsområde redan av den anledningen att de över huvud taget inte är behöriga myndigheter. Någon närmare bedömning av syftet med deras personuppgiftsbehandling behöver inte göras.

Polismyndigheten kan vara en behörig myndighet, eftersom det allmänt sett hör till myndighetens uppgifter att förebygga, förhindra och upptäcka brottslig verksamhet, upprätthålla allmän ordning och säkerhet samt utreda och beivra brott. När brotttsdatalagen infördes uttalade regeringen dock att Polismyndigheten inte är en behörig myndighet när den utfärdar eller annars fattar beslut i fråga om pass (prop. 2017/18:232 s. 131 och 429). Riksdagen gav inte uttryck för någon annan uppfattning om detta (jfr Justitieutskottets betänkande Brotttsdatalag, bet. 2017/18:JuU37 och rskr. 2017/18:392).

Bedömningen att Polismyndigheten inte är en behörig myndighet när personuppgifter behandlas i passverksamheten utgår från syftet med behandlingen. När personuppgifter behandlas i passverksamheten är syftet att utfärda pass eller att handlägga andra typer av passärenden i enlighet med passlagen. Personuppgifterna behandlas inte för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Syftet är inte heller att upprätthålla allmän ordning och säkerhet. Eftersom behandlingen har ett syfte som faller utanför brotttsdatalagens tillämpningsområde är Polismyndigheten inte en

behörig myndighet när den agerar i egenskap av passmyndighet. Detta följer av lagens definition av begreppet behörig myndighet.

En följd av denna bedömning är att inte heller lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag) är tillämplig på Polismyndighetens behandling av personuppgifter i passverksamheten. Detta stämmer överens med vad som har gällt tidigare. Varken 1998 eller 2010 års polisdatalag ansågs vara tillämplig i passverksamheten, eftersom den verksamheten inte ansågs utgöra brottsbekämpning i egentlig mening (jfr propositionen Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85 s. 51, 74 f. och 307).

Det står alltså klart att varken Polismyndigheten, ambassaderna, konsulaten eller Utrikesdepartementet ska tillämpa brottsdatalagen vid sin behandling av personuppgifter inom passverksamheten.

Det finns ändå beröringspunkter med brottsbekämpningen

Den bedömning som har gjorts ovan kan behöva utvecklas något, eftersom det trots allt finns flera beröringspunkter mellan å ena sidan passverksamheten och å andra sidan den brottsbekämpning, lagföring och straffverkställighet som Polismyndigheten och andra myndigheter ansvarar för. Ett exempel är att passmyndigheterna hämtar in information om bl.a. brottsmisstankar och straffrättsliga påföljder vid sin handläggning av passärenden, för att kunna avgöra om det finns hinder mot att utfärda pass eller skäl att återkalla pass. Det förekommer också att personuppgifter från passverksamheten används i polisens och vissa andra myndigheters brottsbekämpande verksamhet. Som utvecklas nedan bedöms brottsdatalagen ändå inte gälla vid behandlingen av personuppgifter i passverksamheten.

Det saknar betydelse att Polismyndigheten är en passmyndighet

Till att börja med saknar det betydelse att just Polismyndigheten är en passmyndighet. Detta har nämnts ovan men kan behöva förklaras närmare. Av förarbetena till brottsdatalagen framgår tydligt att en och samma myndighet kan vara både behörig och inte behörig i brottsdatalagens mening, beroende på syftet med behandlingen av personuppgifter (prop. 2017/18:232 s. 429 f.). Att passärenden

handläggs av Polismyndigheten medför därför inte i sig att lagen är tillämplig. Det är syftet med behandlingen som är avgörande och när det gäller passärenden är syftet inte att bekämpa eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Passverksamheten är en allmän förvaltningsuppgift som Polismyndigheten har vid sidan av brottsbekämpningen och när de dåvarande polismyndigheterna tog över passverksamheten från länsstyrelserna berodde det inte på att den ansågs ha något samband med brottsbekämpningen. Skälet för att föra över passverksamheten var i stället att polismyndigheterna bedömdes kunna erbjuda en bättre service för allmänheten och att verksamheten hade ett nära samband med gränskontroll och gränsövervakning (jfr avsnitt 3.2.4).

Det saknar betydelse att uppgifter om brott behandlas

En passansökan ska i regel avslås bl.a. när sökanden är anhållen eller häktad och i vissa fall när sökanden är dömd till en frihetsberövande påföljd eller avtjänar ett fängelsestraff (jfr avsnitt 3.2.6). När en passansökan registreras sker därför en automatisk kontroll mot bl.a. misstankeregistret, belastningsregistret och kriminalvårdsregistret. Om sökanden förekommer i något av dessa register undersöks saken närmare av Polismyndigheten genom slagningar i registret i fråga. Uppgifter om lagöverträdelser kan behöva hämtas in och behandlas även i ärenden som gäller återkallelse av ett redan utfärdat pass.

Den omständigheten att en myndighet får tillgång till domar eller uppgifter ur belastningsregistret eller misstankeregistret för en viss prövning innebär inte utan vidare att myndigheten blir behörig i brottsdatalagens mening (prop. 2017/18:232 s. 113 och 430). Det är återigen myndighetens uppdrag och syftet med behandlingen av personuppgifter som är avgörande. Att passmyndigheterna får tillgång till uppgifter om brott och brottsmisstankar för att pröva passärenden medför därför inte att brottsdatalagen blir tillämplig.

Flera av bestämmelserna om passhinder och återkallelse syftar i grunden onekligen till att underlätta brottsbekämpning, lagföring eller straffverkställighet. Genom att vissa brottsmisstänkta eller brottsdömda nekas pass eller fråntas sina pass hindras de från att lämna landet och kan därigenom lagföras eller avtjäna sina straff. Att vissa bestämmelser i passlagen har detta bakomliggande syfte

medför emellertid inte att brottsdatalagen blir tillämplig. Det direkta syftet med behandlingen av personuppgifter är fortfarande endast att handlägga passärenden i enlighet med passlagens regler. I den verksamheten har Polismyndigheten, ambassaderna, konsulaten och Utrikesdepartementet inget brottsbekämpande uppdrag. De har inte heller uppgifter som avser verkställighet av straffrättsliga påföljder.

Det saknar betydelse att uppgifter används för brottsbekämpning

Personuppgifter i passärenden och i passregistret används inte bara i passverksamheten. Uppgifterna, inte minst fotografierna, används även av Polismyndigheten vid exempelvis fotokonfrontationer och som ett led i spaningsarbete. Passfotografierna lämnas också ut till bl.a. Ekobrottsmyndigheten (jfr avsnitt 3.3.5). Personuppgifterna i passverksamheten används alltså inom bl.a. brottsbekämpningen.

Det står klart att brottsdatalagen gäller när Polismyndigheten eller en annan behörig myndighet behandlar personuppgifter från passverksamheten för brottsbekämpande syften. Polismyndigheten uppträder i dessa fall inte som passmyndighet och det är inte längre fråga om passverksamhet, dvs. verksamhet som regleras i passlagen. Personuppgifterna lämnar i stället passverksamheten och behandlas för ett nytt ändamål i form av brottsbekämpning. I rättslig mening är det alltså fråga om behandling för ett nytt ändamål, och i vissa fall ett utlämnande, av uppgifter som har samlats in i passverksamheten.

Att personuppgifter i passverksamheten på detta sätt lämnas ut eller behandlas för brottsbekämpande syften leder till flera frågor. Det medför emellertid inte att den personuppgiftsbehandling som utförs av passmyndigheterna inom ramen för passverksamheten omfattas av brottsdatalagen. Ambassaderna och konsulaten har som framgått inget brottsbekämpande uppdrag och det har inte heller Polismyndigheten när den agerar i egenskap av passmyndighet. Den personuppgiftsbehandling som utförs när uppgifterna lämnas ut eller överförs till en brottsbekämpande verksamhet omfattas därför inte av brottsdatalagen. Brottsdatalagen blir tillämplig först när den andra myndigheten, eller den brottsbekämpande enheten inom Polismyndigheten, behandlar uppgifterna för det nya ändamålet. Olika regelverk ska alltså tillämpas av å ena sidan den som lämnar ut eller överför uppgifterna och å andra sidan den som tar emot dem.

Detta synsätt har stöd både i förarbetena till brottsdatalagen och i förarbetena till 2010 års polisdatalag (SOU 2017:29 s. 186 f., prop. 2017/18:232 s. 111 och 430 samt prop. 2009/10:85 s. 307).

Frågan om brottsdatalagen gäller för utlämnande eller överföring av uppgifter till brottsbekämpningen ska skiljas från frågan om uppgifter från passverksamheten över huvud taget bör få användas på det sättet. Den frågan, som gäller finalitetsprincipens tillämpning på uppgifter i passverksamheten, behandlas i avsnitt 6.

Det saknar betydelse att Polismyndigheten ansvarar för passkontroller

Passlagen innehåller inte bara bestämmelser om utfärdande och återkallelse av pass. Lagen reglerar också passkontroller vid utresa ur eller inresa i Sverige (jfr avsnitt 3.2.7). Polismyndigheten är den myndighet som ska se till att bestämmelserna följs, dvs. att svenska medborgare som reser ut ur landet har med sig ett giltigt pass när detta krävs och att svenska medborgare som reser in i landet har med sig ett pass eller kan styrka sitt svenska medborgarskap på annat sätt.

Kontrollverksamhet av det aktuella slaget har normalt ansetts falla utanför brottsdatalagens område (prop. 2017/18:232 s. 113 och 430). Frågan saknar dock betydelse här eftersom Polismyndigheten inte uppträder som passmyndighet vid kontrollerna. Bedömningen att brottsdatalagen inte gäller vid passmyndigheternas behandling av personuppgifter påverkas därför inte av passkontrollernas syfte.

5.3 Dataskyddsförordningen är tillämplig

Bedömning: Dataskyddsförordningen gäller när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter inom ramen för passverksamheten. Även dataskyddslagen och förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning gäller vid personuppgiftsbehandlingen.

Den tidigare promemorian innehåller ingen bedömning i frågan.

Remissinstanserna yttrar sig inte i frågan.

Skälen för bedömningen: Dataskyddsförordningen och dess tillämpningsområde har beskrivits tidigare (avsnitt 4.3.3). Som då har angetts ska dataskyddsförordningen för svensk del tillämpas

även när personuppgifter behandlas som ett led i en verksamhet som inte omfattas av unionsrätten (2 kap. 1 § dataskyddslagen).

Den behandling av personuppgifter som passmyndigheterna och Utrikesdepartementet utför omfattas av dataskyddsförordningens materiella tillämpningsområde under förutsättning att behandlingen företas helt eller delvis på automatisk väg eller, om behandlingen är manuell, att uppgifterna ingår i eller kommer att ingå i ett register. Passverksamheten är till stor del datoriserad och behandlingen av personuppgifter företas alltså på automatisk väg. Det finns vissa undantag från förordningens materiella tillämpningsområde, bl.a. för verksamhet av rent privat natur, men dessa är inte aktuella.

Personuppgiftsbehandlingen i passverksamheten omfattas även av dataskyddsförordningens territoriella tillämpningsområde. Detta gäller inte bara Polismyndighetens och Utrikesdepartementets behandling utan också den som utförs av svenska ambassader och konsulat, oavsett om dessa finns inom eller utanför EU (jfr artikel 3.3 i dataskyddsförordningen och 1 kap. 5 § dataskyddslagen).

Dataskyddsförordningen gäller alltså när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter inom ramen för passverksamheten. Det medför att även dataskyddslagen gäller. Tillsammans bildar dataskyddsförordningen och dataskyddslagen, med anslutande föreskrifter i förordning, det generella regelverk som passmyndigheterna och Utrikesdepartementet ska följa när de behandlar personuppgifter inom ramen för sin passverksamhet.

5.4 Personuppgiftsbehandlingen är laglig

Bedömning: Den personuppgiftsbehandling som utförs i passverksamheten har sådan rättslig grund som avses i artikel 6.1 c och e i dataskyddsförordningen, eftersom den är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Den tidigare promemorian innehåller ingen bedömning i frågan. **Remissinstanserna** yttrar sig inte i frågan.

Skälen för bedömningen

Varje personuppgiftsbehandling ska vila på en rättslig grund

Enligt dataskyddsförordningen ska varje personuppgiftsbehandling vila på en rättslig grund. Utan en rättslig grund är behandlingen inte laglig och får inte utföras. Vilken rättslig grund en behandling har är av stor betydelse för vilka typer av kompletterande bestämmelser som kan införas på nationell nivå. Det behöver därför klarläggas om personuppgiftsbehandlingen i passverksamheten har rättslig grund enligt dataskyddsförordningen och vilken grunden i sådana fall är.

De rättsliga grunderna räknas upp i artikel 6.1 i förordningen. Av bestämmelsen framgår att en behandling är laglig endast om och i den mån som åtminstone ett av följande villkor är uppfyllt:

- a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

De rättsliga grunderna är i viss mån överlappande. Flera grunder kan alltså vara tillämpliga avseende en och samma behandling.

I flera av punkterna anges att behandlingen ska vara nödvändig för ett visst ändamål för att den ska vara laglig. Begreppet nödvändig

ska inte tolkas alltför strikt. En behandling kan vara nödvändig exempelvis om den bidrar till att effektivisera tillämpningen av relevanta bestämmelser, dvs. om den leder till effektivitetsvinster. Kravet på att en behandling ska vara nödvändig innebär alltså inte att den måste vara oundgänglig för ett visst ändamål (jfr propositionen Ny dataskyddslag, prop. 2017/18:105 s. 46 f. och 189).

När myndigheter behandlar personuppgifter för att fullgöra sina uppdrag sker det normalt med stöd av den rättsliga grunden i artikel 6.1 e, dvs. att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (prop. 2017/18:105 s. 53 f.). Uppgiften eller myndighetsutövningen ska enligt artikel 6.3 vara fastställd i enlighet med unionsrätten eller den nationella rätten. Det kan handla t.ex. om att en myndighet enligt lag ska utföra en viss uppgift (prop. 2017/18:105 s. 48–52).

Närmare vägledning för tillämpningen av artikel 6.1 c och e finns i dataskyddslagen. Enligt 2 kap. 1 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 c om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Enligt 2 kap. 2 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 e om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Personuppgifter får enligt samma paragraf behandlas med stöd av artikel 6.1 e även om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Utöver kravet på rättslig grund omgärdas varje behandling också av andra krav enligt dataskyddsförordningen. Att behandlingen har rättslig grund är emellertid en grundläggande förutsättning.

Personuppgiftsbehandlingen i passverksamheten har rättslig grund

Den rättsliga grunden för personuppgiftsbehandlingen i passverksamheten finns i första hand i artikel 6.1 e i dataskyddsförordningen.

Alla uppgifter som riksdag eller regering har gett i uppdrag åt statliga myndigheter att utföra anses vara av allmänt intresse. Myndigheternas verksamhet har också stöd i rättsordningen på det sätt som krävs enligt dataskyddsförordningen (prop. 2017/18:105 s. 56–58). Passverksamheten är reglerad i passlagen och passförordningen. För att kunna utföra sina uppgifter enligt dessa författningar på ett effektivt sätt behöver passmyndigheterna och Utrikesdepartementet behandla personuppgifter. Behandlingen är alltså nödvändig för att utföra en uppgift av allmänt intresse. Det gäller både den behandling som sker inom ramen för enskilda passärenden och den som sker i Polismyndighetens register. Handläggningen av passärenden innefattar vidare myndighetsutövning och personuppgiftsbehandlingen är därför nödvändig även som ett led i myndighetsutövning.

I några fall kan behandlingen ha stöd även i artikel 6.1 c, för att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse. Det kan gälla t.ex. när personuppgifter lämnas ut enligt offentlighetsprincipen. Skyldigheten att lämna ut allmänna handlingar har nämligen betraktats som en rättslig skyldighet. Det kan vidare argumenteras för att skyldigheten att föra ett visst register, som passregistret, är en rättslig förpliktelse (jfr prop. 2017/18:105 s. 53).

5.5 Närmare regler är tillåtna och behövs

Bedömning: Dataskyddsförordningen ger utrymme för närmare bestämmelser om personuppgiftsbehandling i passverksamheten. Sådana bestämmelser behövs för att säkerställa en ändamålsenlig och effektiv verksamhet och ett starkt skydd för den personliga integriteten. De närmare bestämmelser om behandlingen som i dag finns i passlagen och passförordningen är inte tillräckliga.

Den tidigare promemorian innehåller ingen bedömning i fråga om utrymmet för bestämmelser på nationell nivå. När det gäller behovet av närmare bestämmelser om personuppgiftsbehandlingen överensstämmer promemorians bedömning med bedömningen här.

Remissinstanserna tillstyrker eller har inga invändningar mot bedömningen att personuppgiftsbehandlingen i passverksamheten bör regleras närmare. *Datainspektionen* välkomnar en närmare reglering och anger att de bestämmelser som i dag finns i passlagen

och passförordningen inte uppfyller de krav som bör ställas på en författningsreglering till skydd för den personliga integriteten. *Förvaltningsrätten i Stockholm* har förståelse för bedömningen att det behövs mer utförliga och moderna regler om behandlingen av personuppgifter i passverksamheten, mot bakgrund av det stora antalet registrerade i passregistret och personuppgifternas karaktär.

Skälen för bedömningen

De bestämmelser som finns är allmänt hållna

Det finns ingen särskild registerförfattning för passverksamheten. Passlagen och passförordningen innehåller för sin del bara några få bestämmelser om behandling av personuppgifter. Av dessa framgår bl.a. att Polismyndigheten ska föra ett passregister och att vissa uppgifter – fingeravtryck och biometriska data – ska förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Vad passregistret får innehålla eller hur personuppgifter i övrigt ska behandlas framgår dock inte av passlagen eller passförordningen.

Vid sidan av de enstaka bestämmelserna i passlagstiftningen ska passmyndigheterna och Utrikesdepartementet följa de allmänna bestämmelserna i dataskyddsförordningen och dataskyddslagen. Dessa gäller dock generellt, för en rad olika samhällssektorer, och är av naturliga skäl inte anpassade särskilt för passverksamheten.

Den fråga som nu ska bedömas är om dataskyddsförordningen ger utrymme för närmare bestämmelser om hur personuppgifter får behandlas i passverksamheten och om sådana i så fall behövs.

Det är tillåtet att införa närmare bestämmelser

EU-förordningar ska enligt artikel 288 i fördraget om Europeiska unionens funktionssätt ha allmän giltighet samt vara till alla delar bindande och direkt tillämpliga i varje medlemsstat i EU. Förordningar gäller alltså fullt ut och med samma innehåll inom hela EU och ska inte genomföras i nationell rätt. En medlemsstat kan behålla eller införa nationell lagstiftning på det område som en förordning omfattar endast om förordningen ger utrymme för det.

I svensk rätt har det ofta ansetts nödvändigt med ett särskilt anpassat och reglerat integritetsskydd vid behandling av personuppgifter i offentlig verksamhet. Detta gäller inte minst när det har varit fråga om en omfattande behandling av personuppgifter eller personuppgiftsbehandling som av andra skäl har ansetts särskilt integritetskänslig. En sådan ordning innebär att myndigheterna ges ett tydligt rättsligt stöd för den personuppgiftsbehandling som verksamheten kräver och att skyddet för den personliga integriteten säkerställs i olika typer av offentlig verksamhet. Frågan är vilket utrymme dataskyddsförordningen ger för sådana bestämmelser.

Det kan konstateras att dataskyddsförordningen, trots att den är direkt tillämplig, både förutsätter och tillåter nationella bestämmelser som kompletterar delar av förordningen genom olika typer av specificeringar eller undantag. Detta gäller särskilt sådan personuppgiftsbehandling som sker inom den offentliga sektorn.

Av artikel 6.2 i förordningen framgår att medlemsstaterna får införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Detta förutsätter att det är fråga om sådan behandling av personuppgifter som är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c) eller för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e). Personuppgiftsbehandlingen i passverksamheten sker som framgått med stöd av dessa rättsliga grunder.

I enlighet med skäl 8 till förordningen kan medlemsstaterna dessutom under vissa förutsättningar, och i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella reglerna begripliga, införliva delar av förordningen i nationell rätt.

Enligt artikel 6.3 första stycket i förordningen ska de grunder för behandlingen som avses i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Enligt artikel 6.3 andra stycket ska vidare syftet med behandlingen fastställas i den rättsliga grunden eller, i fråga om behandling enligt artikel 6.1 e, vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan enligt artikel 6.3 andra stycket innehålla särskilda

bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen. Bestämmelserna kan avse bl.a. de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas och vilka registrerade som berörs. Bestämmelserna kan vidare gälla vilka enheter som personuppgifterna får lämnas ut till och för vilka ändamål, ändamålsbegränsningar, lagringstider samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling. De särskilda bestämmelserna i den nationella rätten ska i detta avseende uppfylla ett mål av allmänt intresse och vara proportionerliga mot det legitima mål som eftersträvas.

Enligt artikel 23 i förordningen får vissa av de rättigheter och skyldigheter som föreskrivs i förordningen begränsas i nationell rätt. Detta förutsätter dock att begränsningarna sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Det förutsätter också att begränsningen sker för något av de ändamål som anges i artikeln, bl.a. den nationella säkerheten, försvaret och den allmänna säkerheten eller andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse.

Sammanfattningsvis finns det utrymme för att införa eller behålla nationella bestämmelser om myndigheters behandling av personuppgifter, inom de ramar som dataskyddsförordningen ger.

Närmare bestämmelser för passverksamheten behövs

Bristen på en specifik författningsreglering för behandlingen av personuppgifter i passverksamheten har kritiserats. Kritiken har särskilt handlat om att passregistret är bristfälligt reglerat.

Lagrådet har uttalat att den författningsreglering som finns i fråga om passregistret är mycket fragmentarisk och att det behövs en närmare reglering (uttalandet återges i prop. 2004/05:119 s. 95). Integritetsskyddskommittén, som hade i uppdrag att bl.a. kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, har påpekat att regleringen av passregistret består av en enda paragraf i passförordningen. Av paragrafen kan utläsas att det ska finnas ett passregister men inte vilka uppgifter detta register får innehålla eller vad som i övrigt gäller för behandlingen av uppgifter i registret.

Kommittén har vidare påpekat att det är otillfredsställande att ett register som omfattar en så stor del av befolkningen regleras i förordning och inte i lag (betänkandet Skyddet för den personliga integriteten – kartläggning och analys, SOU 2007:22 s. 277, 482 f.).

I promemorian Passdatalag (Ds 2015:44 s. 129 f.) görs bedömningen att det, med hänsyn till det stora antalet personer som är registrerade i passregistret samt omfattningen och karaktären av de uppgifter som behandlas i passverksamheten, finns ett behov av en särskild författningsreglering som både avviker från de allmänna reglerna i personuppgiftslagen och erbjuder ett kompletterande integritetsskydd. Enligt promemorian är det tydligt att de regler i passlagstiftningen som särskilt reglerar personuppgiftsbehandling inte uppfyller de krav som bör ställas på en författningsreglering till skydd för den personliga integriteten. Slutsatsen i promemorian är att en mer utförlig och modern reglering behövs. Remissinstanserna har instämt i den bedömningen eller inte haft några invändningar.

Det kan konstateras att dataskyddsreformen inte har medfört någon avgörande förändring på denna punkt. Behandlingen av personuppgifter i passverksamheten omfattas numera visserligen av dataskyddsförordningen och dataskyddslagen, vilket medför ett relativt starkt skydd för den personliga integriteten, men det saknas alltså bestämmelser som är anpassade för just passverksamheten. Det finns således inga bestämmelser som mer precist reglerar vilka personuppgifter som får behandlas i passregistret, för vilka ändamål personuppgifter i passverksamheten får behandlas eller lämnas ut, vad som gäller i fråga om direktåtkomst och lagringstider osv.

Avsaknaden av närmare bestämmelser är otillfredsställande. Som påpekas i den tidigare promemorian behandlas ett stort antal personuppgifter i passverksamheten. En stor del av befolkningen är registrerad. Även om många av de uppgifter som behandlas framstår som harmlösa behandlas även uppgifter av mer integritetskänsligt slag, som exempelvis fingeravtryck, fotografier och biometriska uppgifter samt uppgifter om hälsa och lagöverträdelser. Som framgått förekommer det vidare att uppgifter behandlas för ändamål som ligger utanför passverksamheten, bl.a. för brottsbekämpning. Allt detta talar för att det behövs så tydliga och precisa bestämmelser som möjligt för personuppgiftsbehandlingen i passverksamheten.

Genom närmare bestämmelser går det att precisera vilken eller vilka myndigheter som har personuppgiftsansvar för behandlingen

av personuppgifter i passverksamheten, vilka personuppgifter som får registreras i passregistret, i vilken utsträckning personuppgifter får användas för brottsbekämpning eller andra ändamål vid sidan av passverksamheten, på vilket sätt personuppgifter får lämnas ut osv. En särskild författningsreglering för personuppgiftsbehandlingen kan på så sätt säkerställa en ändamålsenlig och effektiv verksamhet och ett starkt skydd för den personliga integriteten. En särskild författningsreglering ligger också väl i linje med att regeringen och riksdagen har uttalat att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll normalt sett ska regleras särskilt. De uttalandena behandlas närmare i nästa avsnitt.

Sammanfattningsvis finns det ett behov av närmare bestämmelser om personuppgiftsbehandlingen i passverksamheten, dvs. sådana bestämmelser som kompletterar dataskyddsförordningen. De regler om personuppgiftsbehandling som i dag framgår av passlagen och passförordningen framstår inte som tillräckliga i detta avseende.

5.6 Reglerna bör meddelas genom lag

Bedömning: Bestämmelserna om personuppgiftsbehandling i passverksamheten bör i huvudsak meddelas genom lag.

Den tidigare promemorians bedömning överensstämmer med bedömningen här.

Remissinstanserna tillstyrker eller har inga invändningar mot bedömningen. *Datainspektionen* anser dock, till skillnad från vad som anges i promemorian, att lagform inte bara är lämplig utan också nödvändig. Enligt myndigheten utgör personuppgiftsbehandlingen i passverksamheten ett sådant betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket regeringsformen, med hänsyn till det stora antalet personuppgifter som behandlas och att ett inte obetydligt antal personuppgifter är av integritetskänslig karaktär. *Sveriges advokatsamfund* anför att den enskilde i praktiken inte har någon valmöjlighet när det gäller behandlingen av personuppgifter i passverksamheten. Om den enskilde inte låter myndigheterna behandla hans eller hennes personuppgifter utfärdas inget pass och därmed inskränks den medborgerliga rörelsefriheten.

Skälen för bedömningen

Bestämmelser i regeringsformen

Grundlagens regler om hur normgivningsmakten är fördelad mellan riksdagen och regeringen finns i huvudsak i 8 kap. regeringsformen.

Föreskrifter meddelas av riksdagen genom lag och av regeringen genom förordning. Föreskrifter ska meddelas genom lag bl.a. om de avser skyldigheter för enskilda eller ingrepp i enskildas personliga eller ekonomiska förhållanden (8 kap. 2 § första stycket 2). Kravet på att sådana föreskrifter ska ha lagform är dock inte obligatoriskt. Riksdagen kan bemyndiga regeringen att meddela föreskrifterna. Regeringen får i övrigt meddela bl.a. sådana föreskrifter som inte enligt grundlag ska meddelas av riksdagen (8 kap. 7 §).

Att det allmänna registrerar personuppgifter om enskilda anses inte innebära någon skyldighet för den enskilde. Det har normalt sett inte heller betraktats som ett ingrepp i enskildas personliga förhållanden i den mening som avses i 8 kap. 2 § första stycket 2. Bestämmelser om personuppgiftsbehandling som utförs av statliga myndigheter som lyder under regeringen har därmed i princip ansetts kunna beslutas av regeringen med stöd av dess restkompetens enligt 8 kap. 7 § första stycket 2 (prop. 2017/18:105 s. 26).

Både regeringen och riksdagen har dock uttalat att myndighetsregister som innehåller ett stort antal registrerade och har ett särskilt känsligt innehåll bör regleras i lag, även om lagform inte krävs enligt regeringsformen (jfr regeringens proposition om offentlighet, integritet och ADB, prop. 1990/91:60 s. 58, propositionen Personuppgiftslag, prop. 1997/98:44 s. 41 samt Konstitutionsutskottets betänkanden Offentlighet, integritet och ADB, bet. 1990/91:KU11 s. 11, och Personuppgiftslag, bet. 1997/98:KU18 s. 48).

Sedan 2011 gäller ett utökat grundlagsskydd för den personliga integriteten genom en ny bestämmelse i 2 kap. 6 § andra stycket regeringsformen (jfr avsnitt 4.2.3). Där anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Enligt 2 kap. 20 § regeringsformen får skyddet i vissa fall begränsas genom lag. Det får däremot inte begränsas genom förordning.

Lagform krävs i detta fall inte enligt regeringsformen

I den tidigare promemorian anges att bestämmelser om personuppgiftsbehandling i passverksamheten inte avser skyldigheter för enskilda eller ingrepp i enskildas personliga eller ekonomiska förhållanden i den mening som avses i 8 kap. 2 § första stycket 2 regeringsformen. Ingen av remissinstanserna har invänt mot denna bedömning. Det finns inte heller i övrigt något skäl för att frångå bedömningen. Lagform krävs inte enligt 8 kap. regeringsformen.

Frågan är då om personuppgiftsbehandlingen måste regleras i lag för att den utgör ett sådant betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket regeringsformen.

Det står klart att de uppgifter som behandlas i verksamheten rör enskildas personliga förhållanden i den mening som avses i 2 kap. 6 § andra stycket regeringsformen. Begreppet har samma innebörd som i sekretesslagstiftningen och omfattar bl.a. namn och andra identifikationsuppgifter, adress, familjeförhållanden, hälsa och vandel.

Som *Sveriges advokatsamfund* påpekar måste det ifrågasättas om behandlingen sker med samtycke i egentlig mening. En svensk medborgare måste principiellt sett ha ett pass för att få lämna landet. Den enskilde är alltså tvungen att ansöka om pass, och tillåta att myndigheterna behandlar vissa av hans eller hennes personuppgifter, för att kunna använda sig av sin grundlagsskyddade frihet att lämna landet. Det är inte fråga om något genuint fritt val och förhållandet mellan den enskilde och det allmänna är inte jämlikt. Det är därför svårt att se att behandlingen av personuppgifter sker med ett sådant samtycke som avses i 2 kap. 6 § andra stycket regeringsformen. Som framgått av avsnitt 5.4 är samtycke inte heller den rättsliga grund som behandlingen vilar på enligt dataskyddsförordningen.

I passverksamheten behandlas således uppgifter om enskildas personliga förhållanden utan något egentligt samtycke från de som berörs. Frågan är då om behandlingen innebär övervakning eller kartläggning. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är enligt förarbetena inte åtgärdens huvudsakliga syfte utan vilken effekt den har. Vad som avses med övervakning respektive kartläggning får enligt förarbetena bedömas utifrån vad som enligt normalt språkbruk läggs i dessa begrepp (propositionen En reformerad grundlag, prop. 2009/10:80 s. 250).

Behandlingen av personuppgifter i passverksamheten kan rimligen inte betraktas som övervakning. Frågan är i stället om den kan innefatta kartläggning. Enligt förarbetena är uppgifter i t.ex. databaser med information som är knuten till en myndighets ärendehantering i många fall tillgängliga för myndigheten på ett sådant sätt att lagringen och behandlingen av uppgifterna kan sägas innebära att enskilda kartläggs, även om det huvudsakliga ändamålet med behandlingen är ett helt annat (prop. 2009/10:80 s. 180).

Passregistret får sägas vara utformat som ett personregister. Det innehåller uppgifter om bl.a. namn, personnummer, födelseort, kön och längd. Registret innehåller också ansiktsbilder. När enskilda passärenden handläggs förekommer ytterligare information. Sammantaget får personuppgiftsbehandlingen i passverksamheten därmed anses innefatta en kartläggning av enskildas personliga förhållanden, även om syftet med behandlingen är ett helt annat.

Den avgörande frågan är då om det intrång i den personliga integriteten som behandlingen kan innebära är betydande. Det är bara vissa kvalificerade intrång som omfattas av grundlagsskyddet. Enligt förarbetena bör flera omständigheter vägas in vid den bedömning som ska göras. Stor vikt ska läggas vid uppgifternas karaktär. Ju känsligare uppgifterna är, desto mer ingripande måste hanteringen normalt sett anses vara. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan normalt anses vara mer känslig än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Därutöver kan mängden uppgifter vara en betydelsefull faktor, liksom omfattningen av utlämnande av personuppgifter till andra som sker utan omedelbart stöd av offentlighetsprincipen (prop. 2009/10:80 s. 183 f.).

Omfattningen av personuppgifter i passregistret skulle kunna tala för att intrånget i den enskildes personliga integritet ska anses betydande. I verksamheten förekommer också personuppgifter som är integritetskänsliga, t.ex. information om brottsmisstankar, domar i brottmål, efterlysningar och psykiatrisk tvångsvård. Vissa av dessa uppgifter hämtas in utan den enskildes medverkan. Som framgått behandlas även fingeravtryck, ansiktsbilder och vissa biometriska uppgifter i passverksamheten. I avsnitt 6.10 föreslås dessutom att ansiktsbilder ska få jämföras biometriskt i samband med en ansökan

om pass. Vid bedömningen av intrånget bör det vidare beaktas att personuppgifter från passverksamheten i viss omfattning används i andra sammanhang, bl.a. för brottsbekämpning. Längre fram i denna promemoria (avsnitt 6.12) föreslås att Säkerhetspolisen ska kunna medges direktåtkomst till passregistret för sådana ändamål.

Det måste samtidigt framhållas att syftet med behandlingen av personuppgifter i passverksamheten är att passärenden ska kunna handläggas. Personuppgifter samlas inte in för att brott ska kunna bekämpas eller lagföras. Passverksamheten i sig kan inte betraktas som särskilt integritetskänslig, vilket även *Datainspektionen* påpekar i sitt remissyttrande. Det stora flertalet av personuppgifterna är inte av känslig karaktär och omfattas inte av sekretess. När uppgifter av känsligare karaktär undantagsvis förekommer är det i regel inom ramen för handläggningen av enskilda ärenden. Uppgifter om t.ex. brottsmisstankar, domar i brottmål, efterlysningar och psykiatrisk tvångsvård sparas inte i passregistret, även om de i sällsynta fall kan framgå av beslut i enskilda ärenden. Som framgått sparas inte heller fingeravtryck, eller de biometriska uppgifter som tas fram ur dessa, i passregistret. De förstörs omedelbart när passet har lämnats ut eller passansökan har återkallats eller avslagits. De biometriska uppgifter som har tagits fram ur ansiktsbilder ska enligt förslaget i avsnitt 6.10 endast i begränsad omfattning kunna användas för sökningar.

En viktig aspekt är vidare att den enskilde till övervägande del har kännedom om vilka uppgifter som samlas in och behandlas, eftersom han eller hon har ansökt om pass, låtit sig fotograferas och i övrigt lämnat ifrån sig uppgifter. När det handlar om fotografierna finns det vidare ett starkt sekretesskydd (jfr avsnitt 3.4.4). I avsnitt 7 föreslås att motsvarande sekretess ska gälla för de biometriska uppgifter som har tagits fram ur ansiktsbilderna i passregistret.

Mot denna bakgrund får behandlingen av personuppgifter i passverksamheten visserligen anses utgöra ett intrång i den enskildes personliga integritet, men inte ett så betydande intrång att grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen är tillämpligt. Regeringsformen kräver därmed inte att bestämmelserna om den aktuella personuppgiftsbehandlingen meddelas i form av lag.

Personuppgiftsbehandlingen bör ändå regleras genom lag

Passregistret innehåller uppgifter om ett mycket stort antal personer och som framgått förekommer det integritetskänsliga uppgifter vid handläggningen av passärenden. Det framstår därför som lämpligt att de bestämmelser som föreslås om personuppgiftsbehandlingen i passverksamheten underställs riksdagen och i huvudsak meddelas genom lag, trots att det inte krävs enligt regeringsformen. Det gäller särskilt sådana bestämmelser som reglerar hur personuppgifter kan komma att användas vid sidan av passverksamheten och vilket integritetsintrång som behandlingen i övrigt kan komma att medföra för den enskilde. Något hinder mot att i vissa avseenden komplettera lagbestämmelserna genom föreskrifter på lägre nivå finns dock inte. Det är vanligt förekommande att huvuddragen i en reglering om behandling av personuppgifter på ett visst område meddelas i lag medan kompletterande föreskrifter meddelas i t.ex. förordning.

5.7 En ny registerförfattning bör införas

Förslag: Dataskyddsförordningen och dataskyddslagen ska kompletteras med en passdatalag, dvs. en lag om passmyndigheternas och Utrikesdepartementets behandling av personuppgifter i passverksamheten. Lagen ska kompletteras med en förordning som ska heta passdataförordningen. Lagen och förordningen ska även kunna kompletteras genom föreskrifter på myndighetsnivå.

Den tidigare promemorians förslag överensstämmer i princip med förslaget här. Det föreslås dock att den nya passdatalagen ska gälla utöver personuppgiftslagen, som numera har upphävts.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Datainspektionen* välkomnar förslaget att reglera personuppgiftsbehandlingen i passverksamheten i en särskild lag. *Förvaltningsrätten i Stockholm* har förståelse för bedömningen att det behövs en mer utförlig och modern reglering men anser att de nya bestämmelser som behövs bör införas i passlagen och passförordningen. *Sveriges advokatsamfund* riktar kritik mot flera bedömningar och förslag i promemorian, och kan därför inte ställa sig bakom att förslaget i promemorian läggs till

grund för lagstiftning, men välkomnar i och för sig att det särskilt regleras hur personuppgifter får behandlas i passverksamheten.

Skälen för förslaget: Det står klart att närmare bestämmelser om personuppgiftsbehandlingen i passverksamheten behövs och att dataskyddsförordningen ger utrymme för att införa sådana. Det står också klart att bestämmelserna i huvudsak bör meddelas genom lag.

Frågan är då om de bestämmelser som behövs bör samlas i en särskild registerförfattning eller om de bör tas in i passlagstiftningen, som *Förvaltningsrätten i Stockholm* förespråkar. Något hinder mot att ta in bestämmelserna i passlagstiftningen finns i och för sig inte. Mot den lösningen talar dock att det är fråga om ett relativt stort antal bestämmelser som inte utan vidare kan inordnas i den befintliga strukturen i passlagen och passförordningen. Det framstår därför som ändamålsenligt att samla bestämmelserna i en ny författning.

Lagen kommer att avse dataskydd inom passverksamheten och bör därför få namnet passdatalag. Många registerförfattningar har namngetts på motsvarande vis. Lagen bör innehålla vissa centrala kompletterande bestämmelser till dataskyddsförordningen. Den nya lagen bör i sin tur kompletteras av en ny förordning, som benämns passdataförordning. Kompletterande föreskrifter bör också kunna meddelas på myndighetsnivå. På det sättet undviks att detaljregler som kan komma att behöva ändras ofta måste prövas av riksdagen.

5.8 Något om statliga identitetskort

Passmyndigheterna utfärdar inte bara pass utan också nationella identitetskort. Bestämmelserna om dessa finns i förordningen om nationellt identitetskort. I den tidigare promemorian föreslås en särskild registerförfattning för verksamheten med identitetskort.

Remissinstanserna har inte haft några invändningar mot förslaget om skilda registerförfattningar för verksamheten med pass och verksamheten med nationella identitetskort. Uppdelningen framstår också som rimlig och naturlig, så länge som de nationella identitetskorten finns kvar och regleras i en förordning. Att reglera frågor om personuppgiftsbehandling i en lag när verksamheten i sig är reglerad i en förordning framstår inte som en lämplig ordning.

I betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14) föreslås att förordningen om nationellt identitetskort ska upphävas och ersättas av ett nytt regelverk om statliga identitetskort. Som en del av det regelverket föreslås också särskilda bestämmelser om personuppgiftsbehandlingen i verksamheten.

Om alla förslag till nya författningar genomförs kommer alltså Polismyndigheten och de andra passmyndigheterna att få tillämpa olika bestämmelser om behandling av personuppgifter i två mycket närliggande verksamheter. Så länge bestämmelserna är likartade i sak behöver det inte innebära några särskilda svårigheter. Det kan på sikt ändå finnas skäl att överväga en gemensam reglering, dvs. en lag som gäller för behandling av personuppgifter i både passverksamheten och verksamheten med statliga identitetskort. Ett alternativ kan då vara att anpassa passdatalagen så att den kan gälla även för behandling av personuppgifter i verksamheten med statliga identitetskort.

Det är samtidigt angeläget att den personuppgiftsbehandling som förekommer i passverksamheten regleras närmare utan alltför stor tidsutdräkt. Det går i dag inte heller att veta om förslagen från 2017 års ID-kortsutredning kommer att genomföras. I nuläget bör därför förslaget till passdatalag läggas fram för sig och omfatta endast den behandling av personuppgifter som sker i passverksamheten. Om utredningens förslag inte genomförs kan det bli aktuellt att i ett senare skede se över de bestämmelser om personuppgiftsbehandling som i dag finns i förordningen om nationellt identitetskort.

6 Passdatalagens innehåll

6.1 Syfte och utgångspunkter

Förslag: Passdatalagen ska syfta till att personuppgifter kan behandlas på ett ändamålsenligt sätt i passverksamheten och att människor skyddas mot att deras personliga integritet kränks vid sådan behandling.

Den tidigare promemorians förslag överensstämmer med förslaget här.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget: För att passverksamheten ska fungera på ett tillfredsställande sätt behöver personuppgifter kunna behandlas med hjälp av modern informationsteknik. En sådan automatiserad behandling kan samtidigt innebära en risk för intrång i enskildas personliga integritet. Den nya lagen bör bidra till en väl avvägd balans mellan samhällets befogade krav på en effektiv, rättssäker och välordnad passverksamhet och skyddet för den registrerades personliga integritet. Syftet med lagen bör alltså vara dubbelt.

Detta dubbla syfte bör komma till tydligt uttryck i lagen genom en inledande bestämmelse. En sådan bestämmelse har inte någon självständig rättslig betydelse men den anger utgångspunkterna för regleringen och bidrar till förståelsen för och tolkningen av lagen.

Även i dataskyddsförordningen finns en inledande bestämmelse om regelverkets syfte (artikel 1). Detta utgör inget hinder mot en syftesbestämmelse i passdatalagen. Den föreslagna bestämmelsen är som framgått av upplysningskaraktär. Bestämmelser av motsvarande slag finns i många registerförfattningar och har inte ansetts behöva upphävas eller ändras med anledning av dataskyddsreformen.

En annan viktig utgångspunkt, som inte behöver anges i någon bestämmelse, är att bestämmelserna i lagen bör vara teknikneutrala. Bestämmelserna bör alltså inte knytas till användningen av något visst datorprogram eller liknande. De bör i stället utformas så att de kan tillämpas över tid, oberoende av vilken teknik som används.

6.2 Definitioner av ord och uttryck

Förslag: I passdatalagen ska ordet passverksamhet användas som beteckning för verksamhet enligt passlagen. Övriga ord och uttryck som används ska ha samma betydelse som i passlagen.

Den tidigare promemorians förslag överensstämmer med förslaget här.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Tullverket* anser dock att begreppet passverksamhet bör definieras så att det tydligt framgår att även verksamhet enligt passförordningen omfattas. *Tullverket* menar att Utrikesdepartementets verksamhet med diplomat- och tjänstepass annars riskerar att falla utanför lagens tillämpningsområde.

Skälen för förslaget: Begreppet passverksamhet återfinns inte i passlagen men bör användas i passdatalagen, bl.a. för att avgränsa lagens tillämpningsområde. Begreppet bör avse den verksamhet som bedrivs enligt passlagen, t.ex. utfärdande och återkallelse av pass.

Närmare bestämmelser om olika sorters pass och handläggningen av passärenden finns, som *Tullverket* påpekar, i passförordningen. Närmare bestämmelser finns även i föreskrifter på myndighetsnivå (jfr avsnitt 3.2.2). Dessa bestämmelser har meddelats i anslutning till passlagen och går inte att läsa självständigt. När det talas om verksamhet enligt passlagen omfattas därför även sådan verksamhet som följer av närmare bestämmelser i passförordningen eller i myndighetsföreskrifter. Även den verksamheten har sin grund i passlagen. Det saknas mot den bakgrunden skäl att komplettera definitionen av passverksamhet med en uttrycklig hänvisning till passförordningen. Utrikesdepartementets verksamhet med pass är för övrigt uttryckligt reglerad i 31 § passlagen, där det framgår att departementet under vissa förutsättningar får utfärda pass.

Övriga ord och uttryck som används i passdatalagen bör ha samma betydelse som i passlagen. Det gäller bl.a. begreppet passmyndighet, som används i passlagen (jfr avsnitt 3.2.4).

6.3 Avgränsning av tillämpningsområdet

Förslag: Passdatalagen ska gälla när passmyndigheterna och Regeringskansliet (Utrikesdepartementet) behandlar personuppgifter i passverksamheten. Lagen ska dock gälla endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Den tidigare promemorians förslag överensstämmer med förslaget här.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* anser att det bör förtydligas att kränkande behandling är förbjuden och att vissa säkerhetskrav gäller även vid manuell behandling av personuppgifter som inte ingår i eller kommer att ingå i ett register. Enligt samfundet kan även sådan behandling vara integritetskänslig.

Skälen för förslaget

Tillämpningsområdet måste avgränsas

En grundläggande fråga är vem eller vilka som ska tillämpa den nya lagen och när. Lagens tillämpningsområde måste anges noggrant och avgränsas från andra registerförfattningars tillämpningsområden.

För att bestämma tillämpningsområdet är det lämpligt att ange vilka myndigheter som ska tillämpa lagen och i vilken verksamhet hos dessa myndigheter som lagen ska tillämpas. Det bör även anges vilka typer av personuppgiftsbehandling som lagen ska omfatta.

När det finns utrymme för kompletterande bestämmelser till dataskyddsförordningen finns det ingenting som hindrar att det närmare tillämpningsområdet för dessa anges. I princip samtliga registerförfattningar innehåller bestämmelser av det slaget.

Lagen bör tillämpas av flera myndigheter

Utgångspunkten är att lagen ska tillämpas av passmyndigheterna. Vilka myndigheter som är passmyndigheter framgår av passlagen. Polismyndigheten är passmyndighet inom landet medan vissa beskickningar (ambassader) och konsulat (karriär- eller honorärkonsulat) fullgör uppgifter som passmyndigheter i utlandet. I vilken utsträckning beskickningar och konsulat ska fullgöra uppgifter som passmyndigheter beslutas av Regeringskansliet (jfr avsnitt 3.2.4).

Detta innebär att passdatalagen kommer att tillämpas av flera olika myndigheter. Den kommer att tillämpas av Polismyndigheten i dess egenskap av passmyndighet men också av de ambassader och konsulat som fullgör uppgifter som passmyndigheter i utlandet.

Vid sidan av passmyndigheterna får även Utrikesdepartementet utfärda pass, om det med hänsyn till allmän tjänst som sökanden har eller av annan anledning finns särskilda skäl. Mot den bakgrunden bör även Utrikesdepartementet tillämpa passdatalagen.

Lagen bör tillämpas i myndigheternas passverksamhet

De nämnda myndigheterna har många uppgifter och passdatalagen ska givetvis inte tillämpas i all verksamhet som myndigheterna bedriver. Tillämpningsområdet måste avgränsas till den behandling av personuppgifter som utförs inom ramen för passverksamheten. Med passverksamhet avses, som framgått i föregående avsnitt, all verksamhet som ytterst har sin grund i passlagens bestämmelser.

Passverksamheten går vanligtvis ut på att utfärda pass för svenska medborgare. I vissa undantagsfall kan pass emellertid utfärdas också för utländska medborgare eller för personer vars medborgarskap är oklart. Frågan är om även den verksamheten bör omfattas av den nya lagen eller om det finns skäl att avgränsa tillämpningsområdet till den verksamhet som avser pass för just svenska medborgare.

Enligt 11 § passförordningen får en passmyndighet i utlandet utfärda provisoriskt pass för en sökande som inte kan styrka sitt svenska medborgarskap eller som har förlorat detta utan att förvärva medborgarskap i en annan stat. En passmyndighet i utlandet kan också utfärda en provisorisk resehandling till en medborgare i ett annat EU-land. Utfärdandet av sådana resehandlingar regleras i förordningen om Europeiska unionens provisoriska resehandling

(jfr avsnitt 3.2.5). Den provisoriska resehandlingen räknas enligt 6 § passförordningen som ett särskilt pass i passlagens mening.

Stödet för att utfärda dessa pass för utländska medborgare eller personer vars medborgarskap är oklart finns ytterst i 3 § tredje stycket passlagen, som innehåller ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter i saken. Passen utfärdas av ambassaderna och konsulaten i deras egenskap av passmyndigheter. Det framstår därför som rimligt att den personuppgiftsbehandling som sker i verksamheten omfattas av passdatalagen på samma villkor som annan passverksamhet.

I detta sammanhang bör avgränsningen mot utlänningsdatalagen (2016:27) beröras. Den lagen är tillämplig bl.a. i Migrationsverkets och utlandsmyndigheternas verksamhet som rör utfärdande av resehandlingar (2 § 9). Med detta avses emellertid inte pass enligt passlagstiftningen utan främlingspass och vissa andra resehandlingar enligt utlänningslagstiftningen (propositionen Utlänningsdatalag, prop. 2015/16:65 s. 42 och 107). Utlänningsdatalagen gäller alltså när resehandlingar utfärdas enligt utlänningslagstiftningen medan passdatalagen bör gälla när pass utfärdas enligt passlagstiftningen.

Lagen bör tillämpas på automatiserad behandling och på register

Passdatalagen bör omfatta sådan behandling av personuppgifter som avses i artikel 2.1 i dataskyddsförordningen. Den bör alltså omfatta behandling av personuppgifter som är helt eller delvis automatiserad och behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Detta stämmer i sak överens med vad som gäller enligt i princip alla registerförfattningar. Det saknas skäl att på det sätt som *Sveriges advokatsamfund* förespråkar utvidga tillämpningsområdet genom att låta vissa bestämmelser gälla vid manuell behandling av personuppgifter som inte ingår i eller kommer att ingå i ett register.

Verksamhet som faller utanför tillämpningsområdet

Passdatalagen föreslås alltså gälla när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter i verksamhet enligt passlagen, under förutsättning att behandlingen är helt eller

delvis automatiserad eller, om behandlingen är manuell, att personuppgifterna ingår i eller kommer att ingå i ett register.

Denna utformning av tillämpningsområdet innebär att lagen inte kommer att gälla för personuppgiftsbehandling som utförs av andra myndigheter än passmyndigheterna och Utrikesdepartementet. Det gäller även om verksamheten i och för sig har sin grund i passlagen. Lagen kommer alltså inte att gälla exempelvis när Kriminalvården, Statens institutionsstyrelse eller Socialstyrelsen prövar en fråga om passstillstånd, när en socialnämnd yttrar sig över en passansökan, när en chefsöverläkare anmäler till Polismyndigheten att pass inte får utfärdas utan passstillstånd eller när Kustbevakningen, Tullverket eller Migrationsverket utför passkontroller. När andra myndigheter behandlar personuppgifter har de att följa sina egna regelverk, dvs. dataskyddsförordningen eller brottsdatalagen samt den eller de registerförfattningar som kan gälla för myndighetens verksamhet.

För Polismyndigheten, beskickningarna och konsulaten kommer lagen att gälla bara när de agerar i egenskap av passmyndigheter. Det innebär att lagen inte kommer att gälla när Polismyndigheten utför sådana passkontroller som i och för sig regleras i passlagen men som inte är en uppgift för myndigheten i dess roll som passmyndighet.

Passdatalagen kommer inte heller att gälla när Polismyndigheten behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Polismyndigheten agerar då inte i egenskap av passmyndighet och det är inte heller fråga om verksamhet enligt passlagen. Vid behandling av personuppgifter för dessa ändamål gäller brottsdatalagen och polisens brottsdatalag.

Slutligen kommer passdatalagen inte att gälla när personuppgifter behandlas i passmyndigheternas och Utrikesdepartementets rent administrativa verksamhet avseende t.ex. personal och ekonomi. Den behandlingen saknar koppling till passverksamheten i sak och personuppgifterna har inte samlats in för passhandläggning.

6.4 Förhållandet till andra regler om dataskydd

Förslag: Passdatalagen ska komplettera dataskyddsförordningen i fråga om behandling av personuppgifter. Vid behandling av personuppgifter enligt passdatalagen ska dataskyddslagen och föreskrifter som har meddelats i anslutning till dataskyddslagen gälla, om inte annat följer av passdatalagen eller föreskrifter som har meddelats i anslutning till den lagen.

Den tidigare promemorian innehåller inget förslag i frågan.
Remissinstanserna yttrar sig inte i frågan.

Skälen för förslaget

Förhållandet till dataskyddsförordningen

Dataskyddsförordningen är tillämplig när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter inom ramen för passverksamheten (jfr avsnitt 5.2 och 5.3). Förordningen är direkt tillämplig i alla medlemsstater och utgör en del av den svenska rättsordningen. Passmyndigheterna och Utrikesdepartementet ska alltså tillämpa dataskyddsförordningen direkt i sin passverksamhet.

Även om dataskyddsförordningen är direkt tillämplig tillåter eller förutsätter den att medlemsstaterna i vissa avseenden inför kompletterande bestämmelser, antingen i form av preciseringar eller i form av undantag (jfr avsnitt 5.5). Passdatalagen ska innehålla sådana bestämmelser. Att passdatalagen på detta sätt kompletterar dataskyddsförordningen bör klargöras i en särskild bestämmelse.

Passdatalagens hänvisningar till dataskyddsförordningen bör vara dynamiska. Att hänvisningar är dynamiska innebär att de avser dataskyddsförordningen i den lydelse som gäller vid varje tidpunkt. Genom sådana dynamiska hänvisningar säkerställs det att eventuella ändringar i förordningen får omedelbart genomslag. Det kan dock inte uteslutas att passdatalagen ändå kan behöva ändras i samband med ändringar i förordningen (prop. 2017/18:105 s. 24 f.).

Förhållandet till dataskyddslagen

Bestämmelser som kompletterar dataskyddsförordningen på en generell nivå har samlats i dataskyddslagen. Lagen förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av förordningen. Lagen innehåller också kompletterande bestämmelser i fråga om t.ex. behandling av känsliga personuppgifter, tillsyn, skadestånd och överklagande. Till lagen ansluter förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning.

Dataskyddslagen är subsidiär i förhållande till andra lagar och förordningar. Avvikande bestämmelser i en annan författning, t.ex. en registerförfattning, ska alltså ha företräde framför lagen. Även den förordning som ansluter till dataskyddslagen är subsidiär.

Dataskyddslagens bestämmelser är i stora delar relevanta för passmyndigheternas och Utrikesdepartementets verksamhet. Det gäller bl.a. bestämmelserna om tillsyn, skadestånd och överklagande. Bara i vissa avseenden finns det skäl att införa bestämmelser som kompletterar dataskyddsförordningen men avviker från dataskyddslagen. Dataskyddslagen med anslutande föreskrifter bör därför som utgångspunkt gälla även vid behandling av personuppgifter enligt passdatalagen. I den mån bestämmelser i passdatalagen, eller i föreskrifter som har meddelats i anslutning till lagen, avviker från dataskyddslagen bör dock den avvikande regleringen ha företräde. En bestämmelse som anger detta bör införas i passdatalagen.

6.5 Ansvar för behandlingen

Förslag: Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) ska ansvara för den behandling av personuppgifter som respektive myndighet utför. Polismyndigheten ska ansvara för behandlingen i passregistret och passtillståndsregistret.

Bedömning: Frågor om vem eller vilka som är att betrakta som personuppgiftsbiträden bör inte regleras i lagen.

Den tidigare promemorians förslag och bedömning överensstämmer med förslaget och bedömningen här.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Datainspektionen* framför dock att ett uppdelat personuppgiftsansvar kan komma att medföra vissa

gränsdragningsproblem och att bestämmelsen bör utformas så att det blir tydligt för de registrerade vilken myndighet som ansvarar för behandlingen av personuppgifter. Enligt Datainspektionen kan de registrerade annars få svårt att avgöra vilken myndighet de ska vända sig till om de vill utöva sina rättigheter. Datainspektionen vill också se en fördjupad analys av Migrationsverkets roll i passverksamheten, mot bakgrund av att det i promemorian inte har kunnat klarläggas om ett personuppgiftsbiträdesavtal finns. *Sveriges advokatsamfund* välkomnar att personuppgiftsansvaret förtydligas men anser i likhet med Datainspektionen att ett uppdelat personuppgiftsansvar kan medföra vissa problem. Advokatsamfundet anser att de registrerade bör få veta vilken myndighet de ska vända sig till om de vill utöva sina rättigheter och att myndigheterna därefter sinsemellan bör få avgöra vilken av dem som är ansvarig. Samfundet anser vidare att det bör utredas vilka krav som ska ställas på AB Svenska Pass i egenskap av personuppgiftsbiträde och vilken myndighet som ska ansvara för att ingå ett personuppgiftsbiträdesavtal med AB Svenska Pass.

Skälen för förslaget och bedömningen

Vad innebär personuppgiftsansvar?

En personuppgiftsansvarig är enligt dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Detta framgår av artikel 4.7 i förordningen. Enligt samma artikel är det möjligt för en medlemsstat att i nationell rätt föreskriva vem som är personuppgiftsansvarig för en viss behandling av personuppgifter. En förutsättning för detta är att ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstatens nationella rätt.

Definitionen av begreppet personuppgiftsansvarig är densamma enligt dataskyddsförordningen som enligt personuppgiftslagen. Av särskilda registerförfattningar framgår det ofta vilken eller vilka myndigheter som är personuppgiftsansvarig i en viss verksamhet.

Det är den personuppgiftsansvarige som har ansvaret för att behandlingen av personuppgifter följer dataskyddsförordningen. Förordningen innehåller också en rad konkreta skyldigheter för den personuppgiftsansvarige. Det handlar bl.a. om att lämna information

till de registrerade, att föra ett register över behandlingar, att vidta lämpliga säkerhetsåtgärder, att anmäla personuppgiftsincidenter till tillsynsmyndigheten och att utse dataskyddsombud. Det är till den personuppgiftsansvarige som de registrerade ska vända sig om de exempelvis vill begära rättelse eller radering av personuppgifter.

Vad är ett personuppgiftsbiträde?

Ett personuppgiftsbiträde är enligt artikel 4.8 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet får bara behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige. Den personuppgiftsansvarige och personuppgiftsbiträdet ska reglera hanteringen genom ett avtal. Vissa ytterligare regler om personuppgiftsbiträden finns i artiklarna 28 och 29.

Ansvarsfördelningen bör klargöras

Dataskyddsförordningen tillåter nationella bestämmelser som anger vilken eller vilka myndigheter som ska ha personuppgiftsansvaret för en viss behandling av personuppgifter. Sådana bestämmelser är som framgått mycket vanliga i registerförfattningar. Eftersom flera olika myndigheter är involverade i passverksamheten framstår det som lämpligt att reglera frågan om personuppgiftsansvar i passdatalagen.

Varje myndighet bör ansvara för sin egen behandling

I passverksamheten behandlas personuppgifter vid handläggningen av enskilda passärenden samt i de register som Polismyndigheten ska föra enligt 23 § passförordningen. Frågan är vilken eller vilka myndigheter som bör ansvara för den behandling som utförs.

Som en allmän huvudregel kan anses gälla att den myndighet som utför och styr över en personuppgiftsbehandling också bör ansvara för behandlingen, om det inte finns skäl för något annat (jfr t.ex. prop. 2014/15:148 s. 32–34 och prop. 2015/16:65 s. 55 f.).

De myndigheter som handlägger passärenden är som framgått i första hand Polismyndigheten samt vissa ambassader och konsulat. Dessa är passmyndigheter. Även Utrikesdepartementet, som hör till Regeringskansliet, handlägger passärenden. Utrikesdepartementet är dock inte någon passmyndighet i passlagstiftningens mening.

Bortsett från honorärkonsulaten, som handlägger passärenden i begränsad utsträckning, är varje passmyndighet en fristående myndighet. Det är även Regeringskansliet. Utgångspunkten är att varje myndighet själv bestämmer hur passverksamheten ska bedrivas, inom de ramar som passlagstiftningen ger, och myndigheterna fattar självständiga beslut i passärenden. Detta talar för att varje myndighet själv ska ansvara för den personuppgiftsbehandling som den utför. I fråga om utlandsmyndigheterna är detta också den lösning som har valts när personuppgifter behandlas i den konsulära verksamheten. Av 3 § förordningen (2006:275) om behandling av personuppgifter i utrikesförvaltningens konsulära verksamhet framgår att varje myndighet inom utrikesförvaltningen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Eftersom varje myndighet själv ansvarar för sin passverksamhet framstår det som mindre lämpligt att reglera personuppgiftsansvaret utifrån den bestämmelse om gemensamt personuppgiftsansvar som finns i artikel 26 i dataskyddsförordningen. Den bestämmelsen tar sikte på fall när två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen.

Övervägande skäl talar i stället för att varje myndighet ensam bör ansvara för den behandling av personuppgifter som myndigheten utför vid handläggningen av passärenden. En sådan fördelning av personuppgiftsansvaret kommer i regel att vara den mest begripliga även för den registrerade. Om en registrerad har synpunkter på behandlingen av personuppgifter i ett visst ärende kan det antas att han eller hon vanligtvis kommer att vända sig till den myndighet som tog emot passansökan eller på annat sätt hanterade ärendet. Med den ansvarsfördelning som nu övervägs kommer den myndigheten också att vara personuppgiftsansvarig. Skulle den registrerade någon gång vända sig till fel myndighet har den myndigheten ett ansvar för att hjälpa den enskilde till rätta. Den angivna ansvarsfördelningen bör därmed inte leda till sådana otydligheter eller svårigheter för enskilda som *Datainspektionen* och *Sveriges advokatsamfund* befarar.

Ambassaderna, konsulaten och Utrikesdepartementet använder för närvarande ett datorsystem, RES-UM, som Migrationsverket tillhandahåller. Detta system kommunicerar på olika sätt med det datorsystem som Polismyndigheten använder, RES (jfr avsnitt 3.3). I normalfallet bör det dock inte medföra några svårigheter att avgöra vilken myndighet som rent faktiskt behandlar en viss personuppgift. Att Migrationsverket har inflytande över RES-UM bör inte heller påverka den föreslagna ansvarsfördelningen. Det är vanligt att myndigheter använder sig av datorsystem som andra myndigheter eller företag tillhandahåller (jfr prop. 2014/15:148 s. 32–34).

Sammanfattningsvis bör det alltså införas en bestämmelse som klargör att varje myndighet som utgångspunkt är ansvarig för den behandling av personuppgifter som myndigheten själv utför.

Polismyndigheten bör ansvara för sina register

Av 23 § passförordningen framgår att Polismyndigheten ska föra ett passregister och ett register över omständigheter som avses i 20 § 1 och 3 passlagen, dvs. vissa omständigheter som medför att passstillstånd krävs (jfr avsnitt 3.4.3). I avsnitt 6.9 föreslås att bestämmelsen i passförordningen ska föras över till passdatalagen och att det senare registret ska kallas för passstillståndsregistret. Eftersom Polismyndigheten är registerförande myndighet framstår det som naturligt att myndigheten också är personuppgiftsansvarig för den behandling som sker i registren. Ingen av remissinstanserna invänder mot detta. Det bör alltså införas en bestämmelse i den nya lagen som klargör att Polismyndigheten är personuppgiftsansvarig för den personuppgiftsbehandling som sker i myndighetens register.

Vem som är personuppgiftsbiträde bör inte regleras

Vem som är att betrakta som personuppgiftsbiträde framgår direkt av dataskyddsförordningen. Någon möjlighet att reglera saken i nationell rätt nämns inte i artikel 4.8. Det finns inte heller skäl för en sådan reglering. Vem som anlitas för att t.ex. tillverka pass varierar över tid. Det måste vara upp till de personuppgiftsansvariga och inte till lagstiftaren att bedöma vem som är att anse som biträde och se till att nödvändiga avtal finns. Frågor av det slaget kan ytterst bli

föremål för tillsyn och domstolsprövning. Eftersom det saknas skäl för en reglering saknas det även skäl att utreda dessa frågor närmare.

6.6 När personuppgifter får behandlas

6.6.1 Ändamålsbestämmelser bör införas

Förslag: Den nya lagen ska innehålla bestämmelser som anger för vilka ändamål personuppgifter får behandlas i passverksamheten. Det ska göras en skillnad mellan primära och sekundära ändamål.

Den tidigare promemorians förslag överensstämmer med förslaget här.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget

Allmänt om ändamålsbestämmelser

Personuppgifter ska enligt artikel 5.1 b i dataskyddsförordningen samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Denna princip, som i förordningen kallas för principen om ändamålsbegränsning, gällde även enligt personuppgiftslagen. Det senare ledet i punkten, att personuppgifter som har samlats in för ett visst ändamål inte senare får behandlas på ett sätt som är oförenligt med detta ändamål, kallas vanligtvis för finalitetsprincipen.

Principen om ändamålsbegränsning är central i regelverket om dataskydd. Den innebär att den personuppgiftsansvarige måste göra klart för sig i vilket syfte personuppgifter samlas in. Möjligheten att senare behandla personuppgifterna för andra ändamål är begränsad. Den registrerade skyddas därigenom mot oväntad och integritetskränkande behandling av de personuppgifter som har samlats in.

Dataskyddsförordningen ger utrymme för att införa särskilda ändamålsbestämmelser i nationell rätt. Det anses nämligen vara fråga om sådana specifika bestämmelser som enligt artikel 6.2 och 6.3 anpassar tillämpningen av förordningen och säkerställer en laglig och

rättvis behandling. Att det finns ett utrymme för att införa särskilda ändamålsbestämmelser framgår också av artikel 6.4 och 23.2 a.

I avsaknad av särskilda bestämmelser ska den personuppgiftsansvarige själv bestämma ändamålet med insamlingen av uppgifter. Prövningen av om en ny behandling är förenlig med insamlingsändamålet ska därefter göras direkt med stöd av dataskyddsförordningen. Enligt artikel 6.4 ska flera faktorer beaktas vid den prövningen. Den personuppgiftsansvarige ska något förenklat ta hänsyn till kopplingar mellan ändamålet för insamlingen och det nya ändamålet, förhållandet mellan den registrerade och den personuppgiftsansvarige, personuppgifternas art, eventuella konsekvenser för den registrerade och förekomsten av lämpliga skyddsåtgärder.

Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller vissa statistiska ändamål ska inte anses vara oförenlig med de ursprungliga ändamålen. Detta anges uttryckligen i artikel 5.1 b i förordningen.

Ändamålsbestämmelser i registerförfattningar

Många registerförfattningar innehåller verksamhetsspecifika ändamålsbestämmelser som anger den yttersta ram inom vilken personuppgifter får behandlas. Det är vanligt att ändamålen delas upp i primära och sekundära. Regler om primära ändamål utformas för att tillgodose behoven av att behandla personuppgifter i de berörda myndigheternas egen verksamhet. Personuppgifter får vanligtvis inte samlas in för annat än primära ändamål. Regler om sekundära ändamål tillåter inte att personuppgifter samlas in men medger att uppgifter som redan har samlats in får lämnas ut eller annars behandlas för andra ändamål än det ursprungliga. Både primära och sekundära ändamålsbestämmelser är förenliga med dataskyddsförordningen (se t.ex. propositionen Anpassning av domstolsdatalagen till EU:s dataskyddsförordning, prop. 2017/18:113 s. 118).

Precisering av rättslig grund eller ändamålsbestämmelse?

När 2016 års dataskyddsdirektiv genomfördes uttalade regeringen att gränsen mellan bestämmelser om rättslig grund för behandling och bestämmelser om ändamål för behandling inte är helt klar. Vad

som är bestämmelser om rättsliga grunder och vad som är renodlade ändamålsbestämmelser ansågs ibland ha blandats samman. Det var enligt regeringen därför lämpligt att göra en tydligare skillnad mellan dessa typer av bestämmelser (jfr prop. 2017/18:232 s. 114 f. och propositionen Brottsdatalag – kompletterande lagstiftning, prop. 2017/18:269 s. 138–142). I brottsdatalagen och registerförfattningar på brottsdatalagens område har de primära ändamålsbestämmelserna därför genomgående ersatts med bestämmelser om rättslig grund. Bestämmelserna om sekundära ändamål har tagits bort.

I registerförfattningar på dataskyddsförordningens område finns systemet med primära och sekundära ändamålsbestämmelser kvar. Särskilt i fråga om verksamhet som är tydligt avgränsad och reglerad i sak, som domstolarnas verksamhet, har det godtagits att den rättsliga grunden för behandlingen och de ändamål som personuppgifter får behandlas för ligger nära varandra. Såväl domstolsdatalagen (2015:728) som t.ex. den nya kriminalvårdsdatalagen (2018:1235) innehåller både primära och sekundära ändamålsbestämmelser.

Passdatalagen bör innehålla ändamålsbestämmelser

Passdatalagen bör innehålla ändamålsbestämmelser av det slag som är vanligt i andra registerförfattningar på dataskyddsförordningens område. Därigenom slås det fast vilka ändamål som personuppgifter får behandlas för i passverksamheten. Det innebär för det första att varken passmyndigheterna eller Utrikesdepartementet, eller deras anställda, själva kan besluta om de ändamål för vilka personuppgifter får behandlas i verksamheten. Ändamålsbestämmelserna anger en yttersta ram för behandlingen. För det andra blir det genom sådana verksamhetsspecifika ändamålsbestämmelser tydligare vilka åtgärder som är tillåtna respektive otillåtna. Bestämmelserna i passdatalagen bör utgå från åtskillnaden mellan primära och sekundära ändamål.

6.6.2 Passhandläggning som primärt ändamål

Förslag: Personuppgifter ska få behandlas om det är nödvändigt för handläggning av ärenden om pass. Personuppgifter ska alltså få behandlas bl.a. om det är nödvändigt för att en passmyndighet eller Utrikesdepartementet ska kunna utfärda eller återkalla pass.

Den tidigare promemorians förslag överensstämmer med förslaget här men har en annan lagteknisk utformning. Personuppgifter ska enligt promemorian få behandlas om det behövs för ett antal uppräknade åtgärder, bl.a. för att pröva en ansökan om pass, utfärda ett pass eller återkalla ett pass. Uppräkningen avslutas med en generell punkt som anger att personuppgifter får behandlas om det behövs för att passmyndigheterna och Utrikesdepartementet i övrigt ska kunna fullgöra sina uppgifter enligt passlagen.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Kammarrätten i Göteborg* anser dock att det bör övervägas om inte uppräknningen av olika åtgärder kan ersättas med en bestämmelse som motsvarar den avslutande punkten, dvs. att personuppgifter får behandlas om det behövs för att fullgöra uppgifter enligt passlagen. *Sveriges advokatsamfund* anser tvärtom att den avslutande punkten tvärtom har fått en för obestämd utformning och bör förtydligas, så att den inte möjliggör behandling för ändamål som i praktiken inte är bestämda i förväg.

Skälen för förslaget: Det står klart att passmyndigheterna och Utrikesdepartementet måste kunna behandla personuppgifter när handläggningen av passärenden kräver det. Vilka uppgifter som ska samlas in och hur de ska hanteras vid handläggningen styrs till stor del av de materiella bestämmelserna i passlagen, passförordningen och föreskrifterna på myndighetsnivå. Det framstår varken som möjligt eller meningsfullt att i en ändamålsbestämmelse räkna upp alla handläggningsåtgärder enligt författningarna som kan medföra ett behov av att behandla personuppgifter. Om en sådan uppräknning skulle gå att åstadkomma riskerar den att bli mycket svårtillgänglig. Den kan också komma att behöva ändras om passförfattningarna ändras i sak. Det får därför godtas att det primära ändamål som personuppgifter får behandlas för anges på ett allmänt hållt sätt.

Bestämmelsen bör därmed utformas så att personuppgifter får behandlas om det är nödvändigt för handläggning av ärenden om

pass. Den formuleringen täcker in all behandling av personuppgifter som behövs för att passärenden ska kunna handläggas, oavsett om det enskilda ärendet gäller prövning av en passansökan, återkallelse eller indragning av ett pass eller något annat. Dessutom omfattas alla åtgärder som är nödvändiga att vidta i ett ärende. Exempel på sådana åtgärder är mottagande av uppgifter, diarieföring, kommunicering, sökning, läsning och expediering. Formuleringen täcker också in behandling som inte har koppling till ett konkret ärende men som är nödvändig för att det ska gå att ta emot och hantera t.ex. en anmälan om att passtillstånd krävs för en person. Även sådan behandling är nödvändig för handläggningen av passärenden, eftersom uppgiften krävs för att det senare ska gå att avgöra om pass kan utfärdas.

Att behandlingen ska vara nödvändig för handläggningen innebär inte att den måste vara oundgänglig. Det unionsrättsliga begreppet nödvändig har inte denna strikta innebörd. Behandlingen kan anses nödvändig och därmed tillåten om den leder till effektivitetsvinster. Att behandlingen skulle kunna ske manuellt, dvs. utan tekniska hjälpmedel, hindrar normalt inte att en automatisk behandling kan anses nödvändig. I dagsläget bör det mer eller mindre regelmässigt anses vara nödvändigt att använda tekniska hjälpmedel och därmed behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller företag (prop. 2017/18:105 s. 46 f. och 189).

Det saknas skäl att tillåta insamling av personuppgifter för andra ändamål än det angivna. Bestämmelsen kommer alltså att innebära en uttömmande reglering av de ändamål som passmyndigheterna och Utrikesdepartementet får samla in personuppgifter för.

Som framgått ovan, och som *Sveriges advokatsamfund* anför, är det primära ändamålet allmänt hållet. Det ligger också nära den huvudsakliga rättsliga grunden för behandlingen av personuppgifter inom passverksamheten, dvs. att behandlingen av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Som angetts ovan är det svårt att komma ifrån detta. Problemet ska heller inte överdrivas. Bestämmelsen innebär att personuppgifter får behandlas bara om det är nödvändigt utifrån reglerna i passlagen, passförordningen och föreskrifterna på myndighetsnivå. Det bör därmed gå att avgöra om de uppgifter som har samlats in är adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Bestämmelsen ger ett tydligt skydd mot

integritetskränkningar genom att den inte medger insamling eller annan behandling som inte behövs för att handlägga passärenden.

6.6.3 Gränskontroll som sekundärt ändamål

Förslag: Personuppgifter som har samlats in för handläggning av passärenden ska även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för gränskontroll. Med gränskontroll avses sådana kontroller av svenska och utländska medborgare som Polismyndigheten ansvarar för enligt passlagen och utlänningslagen.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. Av promemorians förslag framgår inte att det är just Polismyndigheten som får behandla uppgifterna för gränskontroll.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget: Polismyndigheten ansvarar för kontroll av personer som passerar Sveriges gränser eller Schengengränserna.

Kontroll av svenska medborgare regleras i passlagen. Av 5 och 5 a §§ passlagen framgår att Polismyndigheten ska se till att svenska medborgare som reser ut ur landet har med sig ett giltigt pass när detta krävs och att svenska medborgare som reser in i landet har med sig ett pass eller kan styrka sitt svenska medborgarskap på annat sätt. Den som ska ha med sig ett pass ska på begäran lämna över detta till en polisman, eller vissa andra tjänstemän, och låta denne ta hans eller hennes fingeravtryck och ansiktsbild för kontroll av att dessa motsvarar de fingeravtryck och den ansiktsbild som finns i passet.

Kontroll av utländska medborgare regleras i utlänningslagen. Av 9 kap. 1 § utlänningslagen framgår att Polismyndigheten ansvarar för kontroll av personer enligt kodexen om Schengengränserna.

Ordet gränskontroll bör kunna användas som samlingsnamn för de kontroller av svenska och utländska medborgare som Polismyndigheten ansvarar för enligt passlagen och utlänningslagen.

Den personuppgiftsbehandling som sker vid gränskontroll faller utanför passdatalagens tillämpningsområde (jfr avsnitt 6.3). Den regleras i stället av bl.a. utlänningsdatalagen. Det står däremot klart att Polismyndigheten vid gränskontroll behöver kunna läsa och på

andra sätt behandla personuppgifter som finns i passverksamheten. Polismyndigheten behöver t.ex. veta om en person har ett giltigt svenskt pass eller inte. Den behandling som behövs i detta avseende syftar inte till att handlägga ärenden om pass och omfattas därför inte av den primära ändamålsbestämmelsen. Det kan i och för sig argumenteras för att det nya ändamålet utan vidare är förenligt med det ursprungliga, eftersom pass utfärdas just för att kunna fungera som resehandling och visas upp vid kontroll. För att det inte ska råda något tvivel om saken bör det ändå införas en sekundär ändamålsbestämmelse som anger att de personuppgifter som har samlats in för passhandläggning även får behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för gränskontroll. Ingen av remissinstanserna har invänt mot detta. Effektiva gränskontroller är ett legitimt ändamål och behovet av att kunna behandla de personuppgifter som har samlats in i passverksamheten för detta ändamål får anses väga tyngre än den risk för integritetsintrång som behandlingen kan medföra.

I verksamheten med gränskontroll biträds Polismyndigheten av Kustbevakningen, Tullverket och Migrationsverket (5 a § passlagen och 9 kap. 1 § utlänningslagen). Även dessa myndigheter kan behöva kunna läsa och på andra sätt behandla de personuppgifter som finns i passverksamheten. Detta behov bör dock tillgodoses genom andra sekundära ändamålsbestämmelser (se framför allt avsnitt 6.6.5) samt bestämmelser om elektroniskt utlämnande av personuppgifter och uppgiftsskyldighet för Polismyndigheten (avsnitt 6.12 och 6.13).

6.6.4 Brottsbekämpning som sekundärt ändamål

Förslag: Personuppgifter som har samlats in för handläggning av passärenden ska även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

Den tidigare promemorians förslag överensstämmer med förslaget här. Vissa språkliga ändringar har gjorts för att ändamålen ska anges på samma sätt som i polisens brottsdatalag.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* anser dock att det angivna ändamålet är för obestämt. Det medför enligt samfundet att det inte går att förutse hur Polismyndigheten kan komma att använda personuppgifterna. Det kan t.ex. tänkas att myndigheten kommer att använda uppgifterna för att byta till sig information från utländska myndigheter. Hur dessa sedan använder uppgifterna går inte att kontrollera. Enligt samfundet bör ändamålet preciseras. *Säkerhets- och integritetsskyddsnämnden* ifrågasätter inte behovet av att behandla personuppgifter för det angivna ändamålet men anser att intresseavvägningen mellan detta behov och risken för integritetsintrång bör utvecklas. *Säkerhetspolisen* framför att inte bara Polismyndigheten utan också Säkerhetspolisen har ett behov av att behandla personuppgifter som förekommer i passverksamheten i sin brottsförebyggande och brottsbekämpande verksamhet.

Skälen för förslaget: Till Polismyndighetens huvuduppgifter hör att förebygga, förhindra och upptäcka brottslig verksamhet, utreda och lagföra brott samt upprätthålla allmän ordning och säkerhet. I den verksamheten används inte sällan personuppgifter som har samlats in i passverksamheten. Fotografier i passregistret används t.ex. vid fotokonfrontationer och i samband med spaningsarbete.

Det finns goda skäl för att Polismyndigheten även i framtiden ska kunna använda sig av personuppgifter från passverksamheten för att bekämpa och lagföra brott samt upprätthålla allmän ordning och säkerhet. Utan en specifik ändamålsbestämmelse skulle det kunna uppfattas som oklart om behandling för sådana ändamål är förenlig med det ändamål som personuppgifterna har samlats in för, dvs. handläggning av passärenden. En sekundär ändamålsbestämmelse som uttryckligen tillåter behandling för brottsbekämpning, lagföring och upprätthållande av allmän ordning och säkerhet bör därför övervägas. Som *Säkerhets- och integritetsskyddsnämnden* anger måste behovet av behandling för sådana ändamål därvid vägas mot riskerna för intrång i de registrerades personliga integritet.

Brottsbekämpning, lagföring och upprätthållande av allmän ordning och säkerhet är viktiga samhällsintressen som erkänns även i dataskyddsförordningen (jfr artikel 23.1). Det är uppenbart att Polismyndigheten får avsevärt bättre möjligheter att bekämpa och lagföra brott samt upprätthålla allmän ordning och säkerhet om personuppgifter från passverksamheten kan användas för sådana

ändamål. Det gäller de fotografier av god kvalitet som är sparade i passregistret men också andra personuppgifter som har samlats in.

När det gäller riskerna för den personliga integriteten kan det konstateras att brottsdatalagen och polisens brottsdatalag kommer att gälla om personuppgifter från passverksamheten behandlas för de angivna ändamålen. Ett uttryckligt syfte med dessa lagar är att skydda fysiska personers grundläggande rättigheter och friheter (1 kap. 1 § brottsdatalagen). Behandlingen kommer att omfattas av lagarnas bestämmelser om bl.a. rättslig grund, ändamål, lagringstider och överföring till tredjeland. Behandlingen kommer också att stå under tillsyn av Datainspektionen och Säkerhets- och integritetsskyddsnämnden. En behandling för brottsbekämpande ändamål kommer alltså att omfattas av ett väl utvecklat regelverk till skydd för den enskildes personliga integritet. Den oro som *Sveriges advokatsamfund* ger uttryck för framstår därför inte som befogad.

Det bör vidare beaktas att personuppgifterna i passverksamheten ofta är harmlösa eller i vart fall inte av särskilt integritetskänsligt slag. Uppgifter om brott och brottsmisstankar hämtar Polismyndigheten inte från passverksamheten utan från andra register. Fingeravtryck och sådana biometriska data som tas fram ur fingeravtryck sparas inte i passregistret och någon ändring i det avseendet föreslås inte i denna promemoria. Sannolikt kommer det i praktiken ofta vara fråga om att Polismyndigheten för brottsbekämpande ändamål tar del av de fotografier som finns sparade i passregistret. Senare i detta kapitel (avsnitt 6.11) föreslås det tydliga begränsningar i fråga om möjligheten att utföra sökningar med hjälp av ansiktsbilder.

När risken för integritetsintrång värderas kan det slutligen inte bortses från att flertalet personuppgifter i passverksamheten har samlats in direkt från den registrerade, som i regel har vänt sig till Polismyndigheten med en passansökan. Det kan därför inte komma som en överraskning att Polismyndigheten, med de uppdrag som myndigheten har, har tillgång till de aktuella personuppgifterna.

Vid en samlad bedömning är det rimligt att personuppgifter som har samlats in för passhandläggning även får behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. De angivna ändamålen motsvarar dem i 1 kap. 1 § polisens brottsdatalag.

Som *Säkerhetspolisen* påpekar kan även andra myndigheter som har till uppgift att bekämpa och lagföra brott behöva ta del av eller på andra sätt behandla de personuppgifter som finns inom passverksamheten. Detta behov bör dock tillgodoses genom andra sekundära ändamålsbestämmelser (se framför allt avsnitt 6.6.5) samt bestämmelser om elektroniskt utlämnande av personuppgifter och uppgiftsskyldighet för Polismyndigheten (avsnitt 6.12 och 6.13).

6.6.5 Uppgiftslämnande som sekundärt ändamål

Förslag: Personuppgifter som har samlats in för handläggning av passärenden ska även få behandlas om det är nödvändigt för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Den tidigare promemorians förslag överensstämmer med förslaget här.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget: Det finns situationer då passmyndigheterna och Utrikesdepartementet behöver kunna behandla personuppgifter som har samlats in för handläggning av passärenden för att lämna ut dessa till andra myndigheter eller till enskilda. En bestämmelse som uttryckligen tillåter behandling för sådana ändamål bör införas.

En allmän förutsättning för sådan behandling som utförs för utlämnande av uppgifter till andra bör vara att uppgiftslämnandet sker i överensstämmelse med lag eller förordning, dvs. med stöd av bestämmelser som påbjuder eller tillåter utlämnande. När regler som påbjuder eller tillåter utlämnande har införts får det förutsättas att det har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, samt att man vid den avvägningen har funnit att uppgiften ska eller får lämnas ut (jfr propositionen Patientdatalag m.m., prop. 2007/08:126 s. 60 och propositionen Domstolsdatalag, prop. 2014/15:148 s. 41).

Passmyndigheterna och Utrikesdepartementet kan enligt olika författningsbestämmelser vara skyldiga att lämna ut uppgifter. Ett exempel är den bestämmelse som i dag finns i 23 § andra stycket passförordningen. Där anges att Polismyndigheten på begäran ska

lämna ut ett fotografi från passregistret till vissa myndigheter. Ytterligare regler om uppgiftsskyldighet föreslås i avsnitt 6.13.

När det gäller uppgifter som inte omfattas av sekretess finns det en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter, om det inte skulle hindra arbetets behöriga gång (6 kap. 5 § offentlighets- och sekretesslagen). Bortsett från fotografier är uppgifterna i passverksamheten normalt sett offentliga (jfr avsnitt 3.4.4). Det innebär att passmyndigheterna och Utrikesdepartementet är skyldiga att lämna ut uppgifterna till en myndighet som begär det, om det inte hindrar arbetets gång.

En myndighet ska dessutom, på begäran av en enskild, lämna uppgift ur en allmän handling som förvaras hos myndigheten om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång (6 kap. 4 § offentlighets- och sekretesslagen).

Det finns vidare situationer när det inte finns någon uttrycklig skyldighet att lämna uppgifter men där det ändå kan anses påbjudet eller önskvärt att passmyndigheterna och Utrikesdepartementet lämnar uppgifter till andra myndigheter eller till enskilda. Det kan t.ex. vara fråga om åtgärder som vidtas för att fullgöra den allmänna serviceskyldigheten gentemot enskilda (prop. 2014/15:148 s. 41 f.).

Det kan möjligen ifrågasättas om det behövs en bestämmelse som tillåter behandling av personuppgifter för dessa fall av utlämnande eller om det räcker att uppgiftsskyldigheten i sig är reglerad. För att det inte ska råda något tvivel om saken, och för att alla olika former av uppgiftslämnande ska omfattas, bör det ändå införas en sekundär ändamålsbestämmelse som anger att uppgifter som har samlats in för passhandläggning får behandlas också för uppgiftslämnande som sker i enlighet med gällande lagar och förordningar. I vilken mån utlämnandet ska få ske elektroniskt behandlas i avsnitt 6.12.

Det bör i detta sammanhang framhållas att passdatalagen aldrig kan förhindra sådana åtgärder som är nödvändiga för att leva upp till offentlighetsprincipen enligt tryckfrihetsförordningen. Grundlag har alltid företräde framför vanlig lag. Allmänna handlingar som inte omfattas av sekretess ska alltid lämnas ut, även om formen för detta utlämnande kan påverkas av bestämmelserna om behandling av personuppgifter (jfr avsnitt 6.12 om elektroniskt utlämnande).

6.6.6 Övriga sekundära ändamål

Förslag: Personuppgifter som har samlats in för handläggning av passärenden ska även få behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Den tidigare promemorians förslag överensstämmer med förslaget här men bygger på regleringen i personuppgiftslagen.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* anser dock att det är problematiskt att de ändamål som anges i lagen inte är uttömmande. Det riskerar enligt advokatsamfundet att medföra en okontrollerad spridning och behandling av uppgifter, på ett sätt som inte är avsett och som äventyrar den personliga integriteten.

Skälen för förslaget: Personuppgifter som har samlats in för handläggning av passärenden bör även få behandlas för vissa andra sekundära ändamål än de som har angetts ovan. Uppgifterna bör bl.a. få behandlas om det behövs för arkivändamål av allmänt intresse. För att möjliggöra detta bör det införas en bestämmelse som anger att personuppgifter som behandlas för det primära ändamålet, alltså handläggning av passärenden, även får behandlas för andra ändamål under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det primära ändamålet. Någon uttrycklig hänvisning till artikel 5.1 b i dataskyddsförordningen, som ger uttryck för denna finalitetsprincip, är inte nödvändig. Det kommer ändå stå klart att personuppgifter får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1 i förordningen, eftersom det redan av artikel 5.1 b i förordningen framgår att behandling för de ändamålen inte ska anses vara oförenlig med de ursprungliga ändamålen.

Som *Sveriges advokatsamfund* påpekar innebär den föreslagna bestämmelsen att de sekundära ändamålen inte anges uttömmande. En nackdel med en sådan reglering är att det kan bli mindre tydligt vilken personuppgiftsbehandling som får förekomma med stöd av passdatalagen. Finalitetsprincipen innebär dock ett integritetsskydd i sig eftersom den förbjuder sådan behandling som är oförenlig med ursprungsändamålet. Vad som ska beaktas när det bedöms om en behandling för nya ändamål är förenlig med det ursprungliga

ändamålet anges i artikel 6.4 i dataskyddsförordningen (se även skäl 50). Förslaget får mot den bakgrunden anses vara godtagbart ur integritetssynpunkt. Många registerförfattningar har för övrigt sekundära ändamålsbestämmelser som är utformade på samma sätt (se t.ex. 7 § domstolsdatalagen och 4 § kriminalvårdsdatalagen).

6.7 Den registrerades rättigheter

Förslag: Den rätt att invända mot personuppgiftsbehandling som framgår av artikel 21.1 i dataskyddsförordningen ska inte gälla vid behandling som är tillåten enligt passdatalagen eller föreskrifter som har meddelats i anslutning till passdatalagen.

En passinnehavare ska på samma sätt som i dag ha rätt att hos en passmyndighet kontrollera den information som har sparats i det chip som finns i passet. Den bestämmelse som finns om detta ska föras över från passförordningen till passdataförordningen.

Bedömning: Vid sidan av rätten att invända mot behandling bör den registrerades rättigheter enligt dataskyddsförordningen gälla utan andra undantag än de som följer av dataskyddslagen.

Den tidigare promemorian behandlar inte den registrerades rättigheter enligt dataskyddsförordningen. När det handlar om den registrerades möjlighet att motsätta sig behandling som är tillåten enligt den föreslagna lagen överensstämmer promemorians förslag ändå med förslaget här. Förslagen överensstämmer även i fråga om passinnehavarens rätt att kontrollera viss information i passet.

Remissinstanserna tillstyrker eller har inga invändningar mot förslagen i fråga om rätten att invända mot tillåten behandling och rätten för en passinnehavare att kontrollera information i passet.

Skälen för förslaget och bedömningen

Bestämmelser om den registrerades rättigheter

Vid behandling av personuppgifter har den registrerade ett flertal rättigheter. Dessa regleras i kapitel III i dataskyddsförordningen. Det handlar om rätt till viss information (artiklarna 13 och 14), till registerutdrag (artikel 15) samt till rättelse, radering, begränsning av

behandling och dataportabilitet (artiklarna 16–20). Det finns också bestämmelser om rätten att göra invändningar (artikel 21) och att motsätta sig automatiskt individuellt beslutsfattande (artikel 22).

Den registrerades rättigheter, med motsvarande skyldigheter för den personuppgiftsansvarige, är direkt tillämpliga. Rättigheterna är dock inte absoluta utan kan under vissa förutsättningar begränsas. Detta framgår av artikel 23 i dataskyddsförordningen. Enligt artikeln får begränsningar införas i nationell rätt om begränsningen i fråga sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle, i syfte att säkerställa vissa intressen. En begränsande lagstiftningsåtgärd ska, när det är relevant, innehålla specifika bestämmelser i vissa avseenden, bl.a. om skyddsåtgärder.

Vissa generella begränsningar av den registrerades rättigheter har införts genom dataskyddslagen. Av 5 kap. 1 § dataskyddslagen framgår således att artiklarna 13–15 om information och rätt att få tillgång till personuppgifter inte gäller sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. Bestämmelsen innebär att sådan sekretess eller tystnadsplikt gentemot den registrerade som har stöd i författning, exempelvis i offentlighets- och sekretesslagen, alltid har företräde framför rätten att få information och tillgång till personuppgifter.

Av 5 kap. 2 § dataskyddslagen framgår vidare att rätten att få tillgång till personuppgifter, enligt artikel 15 i förordningen, inte gäller personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Rätten att få tillgång till personuppgifterna gäller dock, enligt andra stycket i paragrafen, om uppgifterna har lämnats ut till tredje part, behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Frågan är om det för passverksamhetens del finns skäl att begränsa den registrerades rättigheter ytterligare, utöver vad som följer av dataskyddslagen. Rätten till dataportabilitet (artikel 20 § dataskyddsförordningen) gäller inte när personuppgifter behandlas i passverksamheten, eftersom behandlingen inte grundar sig på samtycke eller avtal. Den rättigheten behandlas därför inte nedan.

Rätten till information och tillgång till personuppgifter

Vilken information som ska lämnas till den registrerade i samband med att personuppgifter samlas in framgår av artiklarna 13 och 14 i dataskyddsförordningen. Bestämmelserna motsvarar i allt väsentligt de som fanns i personuppgiftslagen, även om det nu föreskrivs att viss ytterligare information ska lämnas. Artikel 15 i förordningen handlar om den registrerades rätt att få tillgång till personuppgifter och motsvarar personuppgiftslagens regler om s.k. registerutdrag.

Rätten till information och tillgång till personuppgifter har som framgått begränsats genom dataskyddslagen när det handlar om sådan information som omfattas av sekretess eller tystnadsplikt i förhållande till den registrerade. Rätten till information och tillgång har också begränsats när det gäller personuppgifter i viss löpande text m.m. Något skäl för ytterligare begränsningar har inte kommit fram. Med de undantag som framgår av dataskyddslagen bör rätten till information och tillgång till personuppgifter således gälla när personuppgifter behandlas inom ramen för passverksamheten.

Enligt 22 a § passförordningen har en passinnehavare rätt att hos en passmyndighet kontrollera den information som har sparats i lagringsmediet i passet. Med detta avses det datachip som finns i varje pass. Bestämmelsen motsvarar artikel 4.1 i rådets förordning nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna. Rättigheten är av ett annat slag än den registrerades rätt att få tillgång till personuppgifter enligt artikel 15 i dataskyddsförordningen och bör därför regleras särskilt även i fortsättningen. Bestämmelsen bör dock föras över från passförordningen till den nya passdataförordning som föreslås.

Rätten till rättelse och radering av personuppgifter

Den registrerade har enligt artikel 16 i dataskyddsförordningen rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade. Med beaktande av ändamålet med behandlingen ska den registrerade även ha rätt att komplettera ofullständiga uppgifter. Det finns inte skäl att begränsa dessa rättigheter när personuppgifter behandlas inom ramen för passverksamheten. Rättigheterna ska alltså gälla.

Enligt artikel 17 i dataskyddsförordningen ska den registrerade under vissa förutsättningar ha rätt att få sina personuppgifter raderade. Rätten till radering gäller dock inte bl.a. om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (artikel 17.3 b). Rätten till radering gäller inte heller i den utsträckning som den sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med sådan behandling som sker för arkivändamål av allmänt intresse (artikel 17.3 d).

Som anges i avsnitt 5.4 är den personuppgiftsbehandling som sker i passverksamheten nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. De personuppgifter som behandlas är därför i regel undantagna från rätten till radering. Det saknas skäl att begränsa rättigheten ytterligare.

Rätten att begära begränsning av behandling

Enligt artikel 18 i dataskyddsförordningen har den registrerade rätt att i vissa fall kräva att behandlingen av personuppgifter begränsas. Med begränsning avses en markering av lagrade personuppgifter i syfte att begränsa behandlingen av dessa i framtiden (artikel 4.3).

Om den registrerade bestrider att personuppgifterna är riktiga eller har gjort en invändning mot behandling av uppgifterna enligt artikel 21.1, ska den personuppgiftsansvarige begränsa behandlingen under den tid som uppgifternas riktighet kontrolleras eller en bedömning görs av vems berättigade skäl som väger tyngst, den registrerades eller den personuppgiftsansvariges (artikel 18.1 a och d). Behandlingen ska även begränsas om den är olaglig eller om personuppgifterna inte längre behövs för ändamålen med behandlingen (artikel 18.1 b och c). Att behandlingen begränsas innebär att personuppgifterna inte får behandlas på något annat sätt än genom att lagras. Det finns dock undantag. Personuppgifterna får enligt artikel 18.2 behandlas även på andra sätt bl.a. om det sker med samtycke eller för ett skäl som rör ett viktigt allmänintresse.

Bestämmelsen i artikel 18.1 d, som reglerar begränsning av behandling när den enskilde har invänt mot behandlingen, får ingen betydelse vid sådan behandling som är tillåten enligt passdatalagen, eftersom rätten att invända mot behandling inte föreslås gälla i dessa fall (se nedan). I övriga fall innebär artikel 18.1 att den registrerade

har rätt att få behandlingen begränsad. Myndigheternas verksamhet inom passdatalagens tillämpningsområde är dock av allmänt intresse. Att det inte sker några avbrott i myndigheternas verksamhet och ärendehandläggning får anses vara ett sådant viktigt allmänintresse som avses i artikel 18.2 och som innebär att myndigheterna kan fortsätta att utföra nödvändig personuppgiftsbehandling även om behandlingen har begränsats. Det saknas därför behov av att införa särskilda inskränkningar av rätten till begränsning av behandling.

Skyldigheten att underrätta tredje man i vissa fall

Om personuppgifter har lämnats ut till någon utomstående, dvs. någon annan än den registrerade, ska den personuppgiftsansvarige normalt sett underrätta mottagaren om personuppgifterna rättas eller raderas eller behandlingen begränsas. Detta anges i artikel 19 i dataskyddsförordningen. Det saknas skäl att begränsa rättigheten.

Rätten att göra invändningar mot behandling

Artikel 21 i dataskyddsförordningen reglerar den registrerades rätt att motsätta sig behandling av personuppgifter. Enligt artikeln ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter som grundar sig på artikel 6.1 e (behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning) eller artikel 6.1 f (en allmän intresseavvägning). Följden av att en invändning görs är att den personuppgiftsansvarige inte längre får behandla de aktuella personuppgifterna, såvida den personuppgiftsansvarige inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

För myndigheternas del innebär regleringen att invändningar endast får göras mot behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (artikel 6.1 e). Myndigheter får nämligen inte grunda sin rätt till behandling av personuppgifter på en allmän intresseavvägning enligt artikel 6.1 f när de fullgör sina uppgifter. Invändningar får inte heller

göras mot personuppgiftsbehandling som utförs med stöd av andra rättsliga grunder. Rätten att göra invändningar gäller alltså inte vid behandling av personuppgifter som är nödvändig t.ex. för att en myndighet ska kunna uppfylla en rättslig förpliktelse (artikel 6.1 c).

Som framgått ges medlemsstaterna genom artikel 23 möjlighet att begränsa vissa av förordningens rättigheter och skyldigheter, däribland rätten att göra invändningar enligt artikel 21. Enligt artikel 23 får en sådan begränsning göras om den sker med respekt för de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle, bl.a. i syfte att säkerställa andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse. En begränsande lagstiftningsåtgärd ska innehålla specifika bestämmelser åtminstone, när det är relevant, avseende bl.a. ändamålen med behandlingen eller kategorierna av behandling och lagringstiden samt tillgängliga skyddsåtgärder.

Det är av stor betydelse att personuppgifter i passverksamheten får behandlas oberoende av den registrerades inställning. Den personuppgiftsbehandling som är tillåten enligt passdatalagen är en förutsättning för att myndigheterna ska kunna utföra sina uppgifter på ett korrekt, rättssäkert och effektivt sätt. Myndigheterna får närmast undantagslöst anses kunna påvisa starka skäl för fortsatt behandling, som väger tyngre än den registrerades intressen i det enskilda fallet. Under sådana förhållanden och för att fullt ut säkerställa att myndigheterna kan behandla personuppgifter när detta krävs bör den registrerade inte ha någon rätt att motsätta sig sådan personuppgiftsbehandling som är tillåten enligt lagen.

Denna begränsning av den registrerades rättigheter får anses utgöra en nödvändig och proportionell åtgärd i syfte att säkerställa ett viktigt mål av allmänt intresse. Passdatalagen innehåller dessutom specifika bestämmelser om bl.a. ändamålen med behandlingen, vilka personuppgifter som får behandlas, tillgången till personuppgifter, sökbegränsningar och lagringstider. Lagen ger tydliga ramar för personuppgiftsbehandlingen och minimerar risken för kränkningar av den registrerades rättigheter och friheter. Begränsningen får därför anses uppfylla de krav som ställs i artikel 23 i förordningen.

Sammanfattningsvis bör det därmed införas en bestämmelse som anger att rätten att göra invändningar enligt artikel 21.1 i dataskyddsförordningen inte gäller vid sådan behandling som är tillåten enligt passdatalagen eller föreskrifter som ansluter till passdatalagen.

Rätten att inte bli föremål för automatiserade beslut

I artikel 22 i dataskyddsförordningen anges att den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Begreppet profilering definieras i artikel 4.4 i förordningen. I korthet avser begreppet varje form av automatisk behandling av personuppgifter som består i att dessa används för att bedöma vissa personliga egenskaper hos en person.

Rättigheten enligt artikel 22 är inte undantagslös. Den gäller t.ex. inte om beslutet tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och begränsade intressen (artikel 22.2 b).

Om beslutet grundar sig på känsliga personuppgifter krävs enligt artikel 22.4 i förordningen att behandlingen av uppgifterna är tillåten enligt artikel 9.2 a eller 9.2 g i förordningen och att lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Exakt hur artikel 22 ska tolkas är inte alldeles klart (jfr t.ex. prop. 2017/18:115 s. 29–31). En tolkning är att artikeln omfattar alla typer av automatiserade beslut. En annan tolkning, som vinner stöd av skäl 71 till förordningen, är att artikeln endast omfattar automatiserade beslut som innefattar profilering. I avsaknad av praxis kan någon säker slutsats inte dras. Några automatiserade beslut som innefattar profilering fattas inte i passverksamheten. I den mån rättigheten i stället avser alla typer av automatiserade beslut finns det i svensk rätt ett allmänt stöd för sådant beslutsfattande, genom 28 § första stycket förvaltningslagen (2017:900). Ett sådant beslutsfattande är omgärdat av olika förvaltningsrättsligt reglerade skyddsåtgärder.

Det finns mot denna bakgrund inte anledning att i passdatalagen införa några särskilda bestämmelser som begränsar den registrerades rättigheter enligt artikel 22 i dataskyddsförordningen.

6.8 Vissa säkerhetsåtgärder

Förslag: Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter. Respektive myndighet ska få meddela närmare föreskrifter om tillgången till personuppgifter. Regeringen eller den myndighet som regeringen bestämmer ska kunna meddela ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Den tidigare promemorians förslag överensstämmer med förslaget här när det gäller tillgången till personuppgifter.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* framför dock att säkerheten för personuppgifter borde ha fått betydligt större uppmärksamhet i promemorian och att säkerhetsfrågorna borde utredas vidare. När det gäller tillgången till personuppgifter anser advokatsamfundet att promemorian inte tillräckligt uppmärksammar vilka konkreta åtgärder som bör vidtas för att uppgifter inte ska bli tillgängliga för tjänstemän som inte behöver dem. Samfundet ifrågasätter om det finns ett behov av tillgång till RES för alla tjänstemän som i dag har det. Enligt samfundet bör det utredas och registreras hur många och vilka som har tillgång till informationen i de berörda systemen.

Skälen för förslaget

Tillgången till personuppgifter

I passverksamheten behandlas en stor mängd personuppgifter. En del av dem är känsliga i rättslig mening eller integritetskänsliga på andra sätt. Det är därför viktigt att motverka att uppgifterna sprids inom myndigheterna till någon som inte är behörig att ta del av dem.

Den personuppgiftsansvarige är enligt artiklarna 24.1 och 32 i dataskyddsförordningen skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med personuppgiftsbehandlingen. Skyldigheten gäller bl.a. uppgifternas tillgänglighet (artikel 25.2). En begränsning av tillgången till personuppgifter är ett sådant specifikt krav på behandlingen som enligt artikel 6.2 får fastställas i

nationell rätt (jfr t.ex. propositionen Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning, prop. 2017/18:254 s. 36).

Det bör mot denna bakgrund införas en bestämmelse som anger att tillgången till personuppgifter inom passmyndigheterna och Utrikesdepartementet ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter. Anställda och andra som deltar i verksamheten får därmed inte ges tillgång till andra eller fler personuppgifter än vad som behövs med hänsyn till deras arbete.

Bestämmelsen bör vara allmänt hållen eftersom det är svårt att på förhand ta ställning till exakt vilken information olika tjänstemän behöver. Det får vara upp till respektive myndighet att analysera sin verksamhet och därefter begränsa tillgången till personuppgifter i enlighet med bestämmelsen. För att kunna precisera vad som ska gälla bör myndigheterna själva få meddela närmare föreskrifter, dvs. verkställighetsföreskrifter, om tillgången till personuppgifter. För att möjliggöra det föreslås bemyndiganden i passdataförordningen.

Tillgången till personuppgifter kan begränsas på olika sätt. Det kan handla om både tekniska och organisatoriska åtgärder. Vilka åtgärder som är lämpligast beror bl.a. på vilka tekniska möjligheter varje myndighet har och hur myndighetens organisation ser ut. Det framstår därför inte som ändamålsenligt att, på det sätt som *Sveriges advokatsamfund* förordar, reglera vilka konkreta åtgärder som ska vidtas för att begränsa tillgången. Vid behov kan myndigheterna själva meddela föreskrifter om detta, med stöd av de bemyndiganden som föreslås. Hur många tjänstemän som ges tillgång till uppgifter av olika slag är ytterst en fråga som kan bli föremål för tillsyn.

Säkerhetsåtgärder i övrigt

Den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med personuppgiftsbehandlingen. Detta framgår, som nämnts ovan, direkt av dataskyddsförordningen.

Det är alltså upp till den personuppgiftsansvarige att analysera vilka risker en behandling av personuppgifter kan medföra och att vidta lämpliga tekniska och organisatoriska åtgärder utifrån den analysen. I denna promemoria föreslås flera bestämmelser som ska bidra till en hög säkerhetsnivå vid behandlingen av personuppgifter

i passverksamheten. Begränsningen av tillgången till personuppgifter är bara ett exempel. Det kan dock inte uteslutas att det i något avseende bör ställas ytterligare eller mer detaljerade krav på tekniska eller organisatoriska åtgärder. Regeringen eller den myndighet som regeringen bestämmer bör därför kunna meddela ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

6.9 Register i passverksamheten

6.9.1 Polismyndigheten bör ha två register

Förslag: Polismyndigheten ska liksom i dag föra ett passregister och ett register över vissa omständigheter som medför att passstillstånd krävs för en person. Bestämmelserna om dessa register ska föras över från passförordningen till passdatalagen. Det senare registret ska kallas passtillståndsregistret. Båda registren ska föras med hjälp av automatiserad behandling.

Den tidigare promemorians förslag överensstämmer med förslaget här. I promemorian används dock inte passtillståndsregistret som benämning för det register som avser passtillstånd.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget

Dagens bestämmelser om register

Polismyndigheten ska i dag, enligt 23 § passförordningen, föra ett passregister och ett register över omständigheter som avses i 20 § 1 och 3 passlagen. De omständigheter som avses är att passtillstånd krävs för den som är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård om (20 § 1) chefsöverläkaren har gjort en anmälan till Polismyndigheten om att pass inte får utfärdas utan ett sådant tillstånd eller (20 § 3) ett tidigare utfärdat pass efter intagningen har återkallats på grund av en framställning från Socialstyrelsen.

Som nämnts tidigare har regleringen av passregistret kritiserats. Det har påtalats att regleringen är fragmentarisk och att det inte framgår vilka uppgifter som får finnas i registret. Det har också

ansetts otillfredsställande att ett register som omfattar en så stor del av befolkningen regleras i förordning och inte i lag. Det finns mot den bakgrunden skäl att se över dagens bestämmelser om register i passverksamheten, för att åstadkomma en förbättrad reglering.

En tydligare och mer ändamålsenlig reglering

De register som Polismyndigheten ska föra enligt passförordningen behövs i passverksamheten. För att passmyndigheterna och Utrikesdepartementet ska kunna fullgöra sina uppgifter enligt passlagen måste det gå att kontrollera t.ex. vilket passinnehav en person har sedan tidigare och om passtillstånd krävs. Registren bör finnas kvar även i fortsättningen. För att förbättra integritetsskyddet bör de emellertid regleras på ett tydligare och utförligare sätt än i dag.

För det första bör registren i allt väsentligt regleras i lag och inte i förordning. Den bestämmelse som ålägger Polismyndigheten att föra registren bör därför föras över från passförordningen till den nya lagen. Det bör så långt som möjligt tydliggöras vilka personer som får registreras och vilka uppgifter om dessa personer som registren får innehålla. Detta är viktigt från integritetssynpunkt.

För det andra bör det förtydligas att båda registren ska föras med hjälp av automatiserad behandling. Registren förs elektroniskt redan i dag men någon uttrycklig bestämmelse i fråga om detta finns inte.

För det tredje bör det införas ett enklare och tydligare namn för registret över omständigheter som avses i 20 § 1 och 3 passlagen. Eftersom registrets ändamål är att visa om passtillstånd krävs är passtillståndsregistret en lämplig beteckning. Passtillstånd kan i och för sig krävas av andra skäl än de som avses i 20 § 1 och 3 passlagen, t.ex. för att sökanden avtjänar ett fängelsestraff, men det nya namnet kommer knappast att leda till några praktiska svårigheter. En enkel och tydlig beteckning kommer tvärtom att bidra till att både enskilda och myndigheter lättare kan förstå registrets syfte och innehåll.

6.9.2 Vad bör passregistret få innehålla?

Förslag: Passregistret ska få innehålla uppgifter om personer som är eller har varit parter i passärenden. Vilka uppgifter som får behandlas om dessa personer ska anges uttömmande i lagen. Vissa preciseringar ska dock göras i passdataförordningen.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. I promemorian föreslås ingen uttrycklig bestämmelse om vilka personer som ska få registreras. Förslagen skiljer sig delvis åt även när det gäller vilka uppgifter registret ska få innehålla.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget

Vilka personer bör få registreras i passregistret?

Dagens bestämmelse i passförordningen klargör inte vilka personer som får registreras i passregistret. Något uttryckligt förslag i den delen finns inte heller i den tidigare promemorian. För att skydda den personliga integriteten bör frågan regleras i den nya lagen.

För att passregistret ska kunna fylla sitt ändamål bör registret innehålla uppgifter om personer som har eller har haft pass. Hur långt bakåt i tiden registret bör sträcka sig behandlas i avsnitt 6.14. Regleringen bör tillåta att även personer som t.ex. har ansökt om pass men fått avslag registreras. Bestämmelsen bör därmed utformas så att passregistret får innehålla uppgifter om alla personer som är eller har varit parter i ett ärende om pass. På det viset omfattas alla personer som har ansökt om pass, oavsett om pass har utfärdats eller inte, liksom andra personer som kan tänkas vara eller ha varit parter i ett passärende. Regleringen bör vara uttömmande. Den bör alltså innebära att inga andra personer än de angivna får registreras.

Vilka uppgifter bör få registreras i passregistret?

Frågan är då vilka uppgifter som bör få registreras i passregistret. Vilka uppgifter som registreras i dag framgår av avsnitt 3.4.3. Det handlar till att börja med om namn, personnummer, födelseort, kön,

längd, bild och namnteckning. Därutöver registreras uppgifter om själva passet (passnummer, passtyp och giltighetstid m.m.) samt uppgifter om passärendet (ärendenummer, ansökningsdatum och utfärdande myndighet m.m.). Fingeravtryck och de biometriska data som kan tas fram ur dessa och ur ansiktsbilden får inte sparas. De uppgifterna ska förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Detta framgår av 6 a § passlagen.

Även utan en särskild reglering skulle det finnas gränser för vilka uppgifter som får registreras. De ändamålsbestämmelser som föreslås innebär att personuppgifter får samlas in endast om det behövs för handläggning av passärenden och att personuppgifter i övrigt får behandlas bara för de ändamål som har angetts. Detta gäller för all behandling av personuppgifter i passverksamheten och behöver inte anges särskilt i de bestämmelser som handlar om passregistret.

Från ett integritetsperspektiv är det ändå lämpligt att specificera vilka uppgifter som får behandlas i registret. Det medför en tydlighet och en transparens för den registrerade. För att passregistret ska kunna fylla sitt ändamål bör följande uppgifter få behandlas:

- namn
- person- eller samordningsnummer
- medborgarskap
- födelseort
- kön
- längd
- ansiktsbilder som har tagits vid passansökningar
- namnteckningar som har lämnats vid passansökningar
- uppgifter i handlingar som har kommit in eller upprättats
- uppgifter om pass och om handläggningen av ärenden om pass.

Därutöver bör passregistret, till skillnad från i dag, även få innehålla de biometriska uppgifter som har tagits fram ur ansiktsbilderna. Detta krävs bl.a. för att säkerställa att ingen får flera pass utfärdade under olika identiteter. Frågan behandlas närmare i avsnitt 6.10.

Uppräkningen bör vara uttömmande. Det hindrar dock inte att den i vissa avseenden preciseras genom närmare föreskrifter på lägre nivå. Sådana föreskrifter bör meddelas i fråga om den avslutande punkten ovan. Av passdataförordningen bör framgå att uppgifter som behandlas enligt den punkten får avse pass som har utfärdats, ärendenummer, beslut som har fattats, andra handläggningsåtgärder och kontaktuppgifter. Därmed kan information om exempelvis passnummer, passtyp, giltighet, giltighetstid, ansökningsdatum och utfärdandedatum sparas i registret. Detaljerade föreskrifter av detta slag bör inte tas in i lagen eftersom de behöver kunna ändras enkelt och smidigt om omständigheterna kräver det. Ett nytt datorsystem kan t.ex. kräva att andra typer av administrativa uppgifter sparas.

6.9.3 Vad bör passtillståndsregistret få innehålla?

Förslag: Passtillståndsregistret ska bara få innehålla de uppgifter som är nödvändiga för att man ska kunna avgöra om en person behöver passtillstånd i vissa fall av psykiatrisk eller rättspsykiatrisk vård.

Den tidigare promemorians förslag överensstämmer inte med förslaget här. I promemorian föreslås att registret bara ska få innehålla uppgifter som avser personnummer samt för- och efternamn.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för förslaget: Jämfört med passregistret, som innehåller uppgifter om en stor del av befolkningen, är passtillståndsregistret begränsat. Sådana anmälningar eller återkallelsebeslut som avses i 20 § 1 och 3 passlagen är i praktiken ovanliga och det förekommer att registret inte innehåller några registreringar alls. Vilka uppgifter som behandlas när någon är registrerad framgår av avsnitt 3.4.3.

I den tidigare promemorian föreslås att registret endast ska få innehålla namn och personnummer. Förslaget bygger såvitt framgår på att den närmare informationen om varför passtillstånd krävs, t.ex. uppgifter i en chefsöverläkares anmälan, förvaras utanför registret.

Passdatalagen bör inte utesluta eller försvåra användningen av modern informationsteknik. Uppgifter om psykiatrisk tvångsvård och rättspsykiatrisk vård omfattas regelmässigt av sekretess när de

förekommer i passverksamheten (jfr avsnitt 3.4.4). Det bör därför vara tillåtet att i passtillståndsregistret behandla de uppgifter som är nödvändiga för att man ska kunna avgöra om det krävs passtillstånd för en person enligt 20 § 1 och 3 passlagen. Därmed kan inte bara namn och personnummer behandlas utan också uppgifter om anmälningar från chefsöverläkare och framställningar från Socialstyrelsen.

Genom hänvisningen till de angivna bestämmelserna i passlagen blir det tillräckligt tydligt vilka personuppgifter som får behandlas i registret. Tillsynsmyndigheten kommer t.ex. att kunna kontrollera om de uppgifter som behandlas är adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Eftersom uppgifterna i registret kan vara integritetskänsliga ställs höga krav på säkerheten vid behandlingen. Det är upp till den personuppgiftsansvarige, dvs. Polismyndigheten, att vidta lämpliga tekniska och organisatoriska åtgärder till skydd för personuppgifterna (jfr avsnitt 6.8).

Med hänsyn till registrets känsliga natur föreslås att inga andra myndigheter än de som handlägger passärenden ska kunna medges direktåtkomst till passtillståndsregistret (jfr avsnitt 6.12).

6.10 Integritetskänsliga uppgifter

6.10.1 Flera frågor behöver analyseras

I passverksamheten behandlas vissa känsliga personuppgifter. Det handlar om vissa biometriska uppgifter, uppgifter om hälsa och olika uppgifter som tillsammans kan avslöja ras eller etniskt ursprung.

I passverksamheten behandlas även andra uppgifter som kan vara integritetskänsliga, trots att de inte utgör känsliga personuppgifter i rättslig mening. Det handlar framför allt om uppgifter som rör lagöverträdelser samt personnummer och samordningsnummer.

Gemensamt för dessa kategorier av personuppgifter är att de har eller kan ges ett särskilt skydd enligt dataskyddsförordningen.

I detta avsnitt finns inledningsvis en redogörelse för regelverket om känsliga personuppgifter. Därefter lämnas vissa förslag om när känsliga personuppgifter bör få behandlas i passverksamheten. Ett särskilt avsnitt ägnas åt behandlingen av biometriska uppgifter, särskilt möjligheten att jämföra ansiktsbilder biometriskt i syfte att kontrollera sökandens identitet och innehav av pass i samband med

en passansökan. Avslutningsvis diskuteras behandlingen av uppgifter om lagöverträdelser samt person- och samordningsnummer.

6.10.2 Regelverket om känsliga personuppgifter

Vad är en känslig personuppgift?

Känsliga personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Som känsliga personuppgifter räknas även genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning. Detta framgår av artikel 9.1 i dataskyddsförordningen. I förordningen används dock inte begreppet känsliga personuppgifter. Beteckningen är i stället ”särskilda kategorier av personuppgifter”. När dataskyddslagen infördes gjordes bedömningen att känsliga personuppgifter var ett så inarbetat begrepp att det borde användas även i den nya lagen, vilket nu framgår av 3 kap. 1 § dataskyddslagen. Känsliga personuppgifter är också det begrepp som används i registerförfattningar.

När får känsliga personuppgifter behandlas?

Utgångspunkten är att känsliga personuppgifter inte får behandlas (artikel 9.1 i dataskyddsförordningen). I regel är det alltså förbjudet att t.ex. samla in, lagra, läsa och lämna ut känsliga personuppgifter.

Flera undantag från huvudregeln finns i artikel 9.2 i förordningen. För myndigheters verksamhet är artikel 9.2 g av särskilt intresse. I den artikeln anges att känsliga personuppgifter får behandlas om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Något utrymme för medlemsstaterna att föreskriva ytterligare undantag från förbudet, utöver de som framgår av artikel 9.2, lämnas inte i förordningen. Däremot får medlemsstaterna behålla eller

införa mer specifika bestämmelser i fråga om behandling som sker med stöd av artikel 6.1 c och e i förordningen, även när det gäller känsliga personuppgifter (artikel 6.2 och skäl 10). Vissa undantag i artikel 9.2 innehåller också uttryckliga hänvisningar till och krav på innehållet i unionsrätten och medlemsstaternas nationella rätt.

En generell bestämmelse som kompletterar artikel 9.2 g finns i 3 kap. 3 § dataskyddslagen (jfr prop. 2017/18:105 s. 86–92 och 193–195. Av bestämmelsen framgår att en myndighet får behandla känsliga personuppgifter med stöd av undantaget i artikeln om (1) uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, (2) behandlingen är nödvändig för handläggningen av ett ärende, eller (3) i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Även 3 kap. 6 och 7 §§ dataskyddslagen är av intresse för myndigheters del. Där anges när känsliga personuppgifter får behandlas för arkivändamål och statistiska ändamål enligt artikel 9.2 j i dataskyddsförordningen.

Dataskyddslagen är subsidiär i förhållande till andra lagar och förordningar. Det går därför att införa bestämmelser som tillåter att myndigheter behandlar känsliga personuppgifter även i andra fall eller under andra förutsättningar än de som anges i dataskyddslagen, under förutsättning att villkoren i artikel 9.2 g eller någon av de andra punkterna i artikel 9.2 i dataskyddsförordningen är uppfyllda. Sådana avvikande bestämmelser finns i flera registerförfattningar.

6.10.3 Känsliga personuppgifter i allmänhet

Förslag: Känsliga personuppgifter ska få behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Trots denna begränsning ska känsliga personuppgifter få behandlas när det är tillåtet enligt de bestämmelser som reglerar innehållet i passregistret och passtillståndsregistret.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. Enligt promemorian ska personuppgifter som avslöjar ras eller etniskt ursprung eller rör hälsa få behandlas om uppgifterna är nödvändiga för handläggningen av ett ärende eller om uppgifterna har lämnats i ett ärende och endast behandlas i löpande text.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* framför dock som en allmän synpunkt att säkerheten för personuppgifter borde ha fått betydligt större uppmärksamhet i promemorian, just på grund av att känsliga uppgifter förekommer i passverksamheten. *Juridiska fakulteten vid Lunds universitet* påpekar att den föreslagna bestämmelsen innehåller ordet ras trots att riksdagen har uttalat att ordet bör ersättas.

Skälen för förslaget

Vilka känsliga personuppgifter behandlas i passverksamheten?

En första fråga att bedöma är vilka känsliga personuppgifter som över huvud taget behandlas inom ramen för passverksamheten.

En typ av känsliga personuppgifter som behandlas regelmässigt är sådana biometriska uppgifter som kan tas fram ur fingeravtryck och ansiktsbilder. Exakt vad som avses med biometriska uppgifter behandlas i avsnitt 6.10.4. Att biometriska uppgifter behandlas i passverksamheten är en följd av bestämmelserna i passlagen och rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna. Ett pass ska enligt dessa bestämmelser innehålla fingeravtryck och ansiktsbild. Fingeravtrycken och ansiktsbilden förutsätts kunna användas för biometriska jämförelser vid passkontroller enligt passlagen.

Även uppgifter om hälsa kan behandlas i passverksamheten. Med uppgifter om hälsa avses enligt artikel 4.15 i dataskyddsförordningen personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus. Uppgifter om hälsa behandlas inte regelmässigt i passverksamheten men det finns ett antal bestämmelser i passlagen som medför att uppgifter som i vart fall indirekt handlar om hälsa behöver behandlas. En passansökan ska exempelvis avslås om sökanden genomgår rättspsykiatrisk vård med särskild utskrivningsprövning. Information om olika former av psykiatrisk vård är rimligen att betrakta som uppgifter om hälsa.

Renodlade uppgifter om ras eller etniskt ursprung behandlas inte i passverksamheten. Däremot behandlas fotografier av enskilda samt uppgifter om bl.a. namn, medborgarskap och födelseort. Sådana

kombinationer av uppgifter kan i vissa fall anses avslöja en persons ras eller etniska ursprung (jfr t.ex. propositionen Genomförande av tredje penningtvättsdirektivet prop. 2008/09:70 s. 142). Med hänsyn till vad *Juridiska fakulteten vid Lunds universitet* framför kan det påpekas att användningen av termen ras i dataskyddsförordningen inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser (skäl 51 till förordningen).

Det kan inte uteslutas att även andra känsliga personuppgifter än de angivna behandlas i passverksamheten, om en enskild av något skäl skulle lämna sådana uppgifter till en passmyndighet eller till Utrikesdepartementet. Passlagstiftningen förutsätter dock inte att ytterligare kategorier av känsliga personuppgifterna behandlas.

Behandlingen är nödvändig för viktiga allmänna intressen

Det allmänna förbudet mot behandling av känsliga personuppgifter gäller som framgått inte om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträfvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande och rättigheter intressen (artikel 9.2 g i dataskyddsförordningen).

En första förutsättning för att undantaget i artikel 9.2 g ska vara tillämpligt är att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Enligt förarbetena till dataskyddslagen torde det stå klart att verksamhet som innefattar myndighetsutövning utgör ett viktigt allmänt intresse. Enligt förarbetena måste det även utanför området för myndighetsutövning anses utgöra ett viktigt allmänt intresse att svenska myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (prop. 2017/18:105 s. 83–85).

Passverksamheten är utan tvivel ett viktigt allmänt intresse. När personuppgifter behandlas för handläggning av passärenden är det alltså fråga om en behandling som är nödvändig med hänsyn till ett viktigt allmänt intresse. Därmed får även känsliga personuppgifter behandlas för detta ändamål, under förutsättning att det finns

bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Personuppgifter som har samlats in för handläggning av ärenden om pass ska enligt förslagen i avsnitt 6.6 få behandlas även för vissa andra ändamål. Det handlar till att börja med om gränskontroll, brottsbekämpning, lagföring och upprätthållande av allmän ordning och säkerhet. Även detta är utan tvivel viktiga allmänna intressen. Samma sak gäller för uppgiftslämnande i överensstämmelse med lag eller förordning. Att myndigheter kan lämna ut personuppgifter när det följer av en författning är ett grundläggande samhällsintresse.

Enligt förslaget ska personuppgifter få behandlas även för andra ändamål, så länge uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket de samlades in. Den föreslagna bestämmelsen ger uttryck för den s.k. finalitetsprincipen. Det kan handla om behandling för t.ex. arkivändamål av allmänt intresse, forskningsändamål eller statistiska ändamål. En noggrann prövning av det nya ändamålets förenlighet med det ursprungliga ska göras och det får därför förutsättas att även den behandling som sker för det nya ändamålet är nödvändig för ett viktigt allmänt intresse.

Sammanfattningsvis får all personuppgiftsbehandling som utförs med stöd av de primära och sekundära ändamålsbestämmelserna anses ske för ett viktigt allmänt intresse i den mening som avses i artikel 9.2 g i dataskyddsförordningen. Därmed får även känsliga personuppgifter behandlas för dessa ändamål, så länge behandlingen är nödvändig för ändamålet och omfattas av regler om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (jfr prop. 2017/18:105 s. 84).

Behandlingen omgärdas av lämpliga och särskilda skyddsåtgärder

Genom det regelverk som föreslås i denna promemoria kommer den registrerades grundläggande rättigheter och intressen att skyddas på flera olika sätt när känsliga personuppgifter behandlas.

De föreslagna ändamålsbestämmelserna innebär till att börja med att myndigheternas utrymme att över huvud taget behandla känsliga personuppgifter i passverksamheten är begränsat. Av den primära ändamålsbestämmelsen följer att personuppgifter får samlas in bara om det är nödvändigt för handläggning av ärenden om pass. Därmed

är det i princip otillåtet att samla in personuppgifter som avslöjar den registrerades politiska åsikter, religiösa eller filosofiska övertygelse eller medlemskap i fackförening, genetiska uppgifter eller uppgifter om den enskildes sexualliv eller sexuella läggning. Sådana uppgifter är i princip aldrig nödvändiga att behandla för att passärenden ska kunna handläggas. Behandlingen är därmed inte heller tillåten.

Vissa biometriska uppgifter, uppgifter om hälsa samt uppgifter som avslöjar ras eller etniskt ursprung kan däremot, som framgått, vara nödvändiga att behandla inom ramen för ett passärende. Om så är fallet får dessa känsliga personuppgifter samlas in. När de väl har samlats in får de behandlas också för de sekundära ändamål som föreslås, bl.a. gränskontroll och brottsbekämpning. Även då finns det dock ett starkt skydd mot integritetsintrång. Vid sidan av de krav som följer direkt av dataskyddsförordningen, t.ex. kravet på en lämplig säkerhetsnivå, föreslås passdatalagen innehålla ett flertal bestämmelser om åtgärder till skydd för den personliga integriteten.

Det föreslås således att personuppgiftsansvaret i verksamheten ska klargöras, så att den registrerade vet vem som bär ansvaret för behandlingen och vem han eller hon ska vända sig till för att t.ex. begära rättelse av personuppgifter. Det föreslås vidare att den interna tillgången till personuppgifter inom myndigheterna ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Vidare föreslås en reglering av vad passregistret och passtillståndsregistret ska få innehålla. I avsnitt 6.11 föreslås olika sökbegränsningar och i avsnitt 6.12 föreslås begränsningar även i fråga om elektroniskt utlämnande av personuppgifter. I avsnitt 6.14 finns förslag om hur länge personuppgifter ska få behandlas och i avsnitt 7 föreslås att vissa sekretessbestämmelser ska ändras, så att både ansiktsbilder och biometriska uppgifter som har tagits fram ur ansiktsbilder ska omfattas av en presumtion för sekretess. Därutöver kommer dataskyddsförordningens och dataskyddslagens regler om bl.a. tillsyn, skadestånd och överklagande att gälla. Sammantaget kommer det därmed att finnas ett omfattande regelverk till skydd för den registrerades grundläggande rättigheter och intressen.

Den behandling av känsliga personuppgifter som kommer att ske med stöd av de föreslagna ändamålsbestämmelserna bedöms därmed vara tillåten enligt artikel 9.2 g i dataskyddsförordningen.

Det bör krävas att behandlingen ska vara absolut nödvändig

Kravet på att en behandling av personuppgifter ska vara nödvändig för ändamålet innebär som framgått inte ett krav på att åtgärden ska vara oundgänglig (jfr avsnitt 6.6.2). Begreppet nödvändig har inte den strikta innebörden. Ett sätt att ytterligare förstärka skyddet för den enskildes personliga integritet när känsliga personuppgifter behandlas är därför att, utöver de åtgärder som har nämnts ovan, ställa särskilt höga krav på behovet av att uppgifterna behandlas.

I flera registerförfattningar anges av denna anledning att känsliga personuppgifter får behandlas bara om det är absolut nödvändigt för ändamålet med behandlingen (se t.ex. 5 § kriminalvårdsdatalagen). För att känsliga personuppgifter ska få behandlas räcker det då inte att behandlingen är nödvändig i dataskyddsförordningens mening, dvs. att den t.ex. effektiviserar handläggningen. Behandlingen måste i stället kunna betecknas som absolut nödvändig, vilket innebär att behovet av behandlingen måste prövas noggrant i varje enskilt fall.

För att motverka risken för integritetsintrång bör ett krav av detta slag gälla även enligt passdatalagen. Det bör alltså införas en bestämmelse som anger att känsliga personuppgifter får behandlas i verksamheten endast om det är absolut nödvändigt för ändamålet med behandlingen. På det viset kommer behovet av att behandla känsliga personuppgifter att behöva prövas särskilt noggrant. Kravet kommer att utgöra ytterligare en sådan åtgärd till skydd för den registrerade som avses i artikel 9.2 g i dataskyddsförordningen.

Känsliga personuppgifter i Polismyndighetens register

Känsliga personuppgifter kommer inte bara att behandlas i enskilda ärenden utan också i passregistret och passtillståndsregistret. Enligt förslaget i denna promemoria ska passregistret få innehålla uppgifter om bl.a. namn, medborgarskap, födelseort, ansiktsbild och, vilket utvecklas i nästa avsnitt, biometriska uppgifter som har tagits fram ur ansiktsbilder. Passregistret kommer alltså att innehålla känsliga personuppgifter i form av vissa biometriska uppgifter samt uppgifter som tillsammans i vissa fall kan avslöja den registrerades ras eller etniska ursprung. Passtillståndsregistret kan komma att innehålla information rörande psykiatrisk vård, dvs. uppgifter om hälsa.

Det kan i och för sig ifrågasättas om inte behandlingen av dessa personuppgifter i passregistret och passtillståndsregistret är absolut nödvändig för handläggning av ärenden om pass. För att det inte ska råda något tvivel om att uppgifterna får behandlas i dessa register, oavsett om det kan anses vara absolut nödvändigt i det enskilda fallet eller inte, bör det införas en bestämmelse som uttryckligen anger att känsliga personuppgifter får behandlas när det är tillåtet enligt bestämmelserna om passregistret och passtillståndsregistret.

Säkerheten vid behandling av känsliga personuppgifter

Vid behandling av känsliga personuppgifter ställs höga krav på säkerhet. De personuppgiftsansvariga har ett långtgående ansvar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en hög säkerhetsnivå. Detta framgår direkt av artikel 32 i dataskyddsförordningen och behöver inte anges i passdatalagen. Att tillgången till personuppgifter ska begränsas till det som var och en inom respektive myndighet behöver för att kunna fullgöra sina arbetsuppgifter har redan behandlats (avsnitt 6.8). Säkerheten är vidare en aspekt av personuppgiftsbehandlingen som kan bli föremål för tillsyn. Något skäl att analysera säkerhetsfrågorna ytterligare, vilket *Sveriges advokatsamfund* förordar, finns inte.

6.10.4 Biometrisk jämförelse av ansiktsbilder

Förslag: Passregistret ska få innehålla biometriska uppgifter som har tagits fram ur den ansiktsbild som tas av sökanden.

När en person ansöker om pass ska den ansiktsbild som tas av personen få användas för sökning i passregistret i syfte att kontrollera sökandens identitet och innehav av pass.

Den tidigare promemorians förslag överensstämmer inte med förslaget här. Ansiktsbilden och de biometriska uppgifter som kan tas fram ur den ska enligt promemorian inte få användas vid sökning. Biometriska uppgifter ska inte heller få sparas i passregistret.

Remissinstanserna: Nästan ingen av remissinstanserna yttrar sig särskilt i frågan. *Polismyndigheten* påpekar dock att möjligheten att biometriskt jämföra senast tagna fotografi med tidigare fotografier

skulle vara ett mycket värdefullt verktyg för att säkerställa identitet i samband med passansökningar. Polismyndigheten anser att man inte genom lagstiftning bör begränsa möjligheten att göra jämförelser i bildinnehållet i passregistret när det behövs i passverksamheten.

Skälen för förslaget

Frågor om biometri

I förra avsnittet har det föreslagits att känsliga personuppgifter, vilket inbegriper biometriska uppgifter, ska få behandlas om det är absolut nödvändigt för handläggning av passärenden eller för något sekundärt ändamål. Enligt förslaget ska känsliga personuppgifter också få behandlas när det är tillåtet enligt bestämmelserna om passregistret eller passstillståndsregistret, oavsett om behandlingen kan betraktas som absolut nödvändig för passhandläggningen eller inte.

Den fråga som *Polismyndigheten* lyfter fram är om biometriska uppgifter därutöver bör få behandlas genom datorstödd jämförelse av ansiktsbilder i samband med en passansökan. För att ta ställning till frågan krävs en analys av begreppet biometriska uppgifter och hur biometriska uppgifter behandlas i passverksamheten i dag.

Vad är en biometrisk uppgift?

En definition av begreppet biometriska uppgifter finns i artikel 4.14 i dataskyddsförordningen. Biometriska uppgifter är personuppgifter som har erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter.

Av skäl 51 till dataskyddsförordningen framgår att behandling av fotografier inte systematiskt bör anses utgöra behandling av känsliga personuppgifter, eftersom fotografier endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.

Begreppet biometriska uppgifter förekommer även i 2016 års dataskyddsdirektiv och definieras där, i artikel 3.13, på samma sätt som i dataskyddsförordningen. När direktivet genomfördes i svensk

rätt, genom brottsdatalagen, angav regeringen följande. Biometri är ett samlingsnamn för automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Tekniken baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras. När det gäller pass är det framför allt mönster av fingeravtryck, ansiktsgeometri och ögats iris som brukar användas, men även regnbågshinna, näthinna, röst, hand, blodkärl, dna eller gång går att använda. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Dessa uppgifter kan användas för att skapa en referensmall eller för att jämföra tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. I direktivets definition av biometriska uppgifter anges ansiktsbilder som ett exempel på sådana uppgifter. Det kan leda tanken till att vanliga fotografier och filmer skulle omfattas av definitionen. Om de inte bearbetas tekniskt genom en särskild metod som syftar till identifiering faller de utanför definitionen. Om de däremot bearbetas i exempelvis ett ansiktigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen. (Prop. 2017/18:232 s. 86, se även s. 150 f. och 435.)

I passlagen används i dag begreppet biometriska data i stället för biometriska uppgifter. Någon skillnad mellan uttrycken finns inte.

När får biometriska uppgifter behandlas?

Biometriska uppgifter räknas som känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen. De får behandlas under samma förutsättningar som andra kategorier av känsliga personuppgifter.

Detta betyder att biometriska uppgifter får behandlas bl.a. om de villkor som anges i artikel 9.2 g i förordningen är uppfyllda, dvs. om en behandling är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilket ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Dagens behandling är absolut nödvändig

Biometriska uppgifter behandlas i passverksamheten redan i dag. Den som ansöker om pass är skyldig att låta sig fotograferas och att lämna sina fingeravtryck. Ansiktsbilden och fingeravtrycken fångas digitalt. Under handläggningen kontrolleras de digitala bilderna tekniskt, för att säkerställa att de duger som underlag för biometrisk jämförelse. Bilderna sparas sedan i ett lagringsmedium i passet. När passet har lämnats ut sparas ansiktsbilden i passregistret, medan fingeravtrycken och de biometriska uppgifter som har tagits fram ur fingeravtrycken och ansiktsbilden förstörs. Vid en passkontroll kan de biometriska uppgifterna behandlas på nytt, men även då förstörs de efter behandlingen. Biometriska uppgifter får inte i något skede användas vid sökning med hjälp av automatiserad behandling.

Behandlingen av biometriska uppgifter i passverksamheten i dag grundar sig på 5 a–6 b §§ passlagen och de bestämmelser som finns i rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna. Behandlingen är absolut nödvändig för handläggningen av passärenden. Ett pass ska som framgått innehålla ansiktsbild och fingeravtryck. Vid en passansökan måste biometriska uppgifter tas fram ur den ansiktsbild och de fingeravtryck som tas, för att verifiera att dessa duger som underlag för den datorstödda jämförelse som ska kunna göras vid en passkontroll (prop. 2004/05:119 s. 22 och prop. 2008/09:132 s. 13).

Eftersom behandlingen är absolut nödvändig för handläggningen av passärenden är den tillåten enligt de bestämmelser om behandling av känsliga personuppgifter som har föreslagits i föregående avsnitt. Det behövs alltså inga särskilda bestämmelser för att de biometriska uppgifter som tas fram ur ansiktsbilder och fingeravtryck ska kunna behandlas på det sätt som sker inom passverksamheten i dag.

Biometriska jämförelser av ansiktsbilder är förbjudna

Dagens bestämmelser innebär att ansiktsbilder inte kan användas på det sätt som Polismyndigheten beskriver. Den ansiktsbild som tas i samband med en passansökan får visserligen sparas i passregistret men de biometriska uppgifter som tas fram ur bilden ska raderas när passet har lämnats ut (6 a § passlagen). Varken ansiktsbilden eller de

biometriska uppgifter som kan tas fram ur bilden får användas vid sökning med hjälp av automatiserad behandling (6 b § passlagen).

En konsekvens av bestämmelserna är att den ansiktsbild som tas vid en passansökan inte får användas för att på teknisk väg, genom en sökning i passregistret, kontrollera om sökanden redan har pass under en annan identitet. Det är inte heller tillåtet att på teknisk väg jämföra den nya bild som tas med tidigare bilder av sökanden. En sådan jämförelse får bara göras okulärt, dvs. utan datorstöd.

Att varken ansiktsbilder eller fingeravtryck får jämföras tekniskt med tidigare tagna ansiktsbilder eller fingeravtryck är ett medvetet val av lagstiftaren. I fråga om ansiktsbilderna ansåg lagstiftaren att dessa skulle få sparas i passregistret men att de biometriska uppgifter som kunde tas fram ur bilderna skulle förstöras när passärendet var avslutat och att varken bilderna eller de biometriska uppgifterna skulle få användas för sökning (prop. 2004/05:119 s. 25). När det gäller fingeravtrycken ansåg lagstiftaren att dessa över huvud taget inte skulle få sparas. Det skulle inte vara möjligt att bygga upp ett separat fingeravtrycksregister med hjälp av de fingeravtryck som lämnas vid passansökningar (prop. 2008/09:132 s. 12 f. och 16).

Förbudet mot biometriska jämförelser leder till problem

Svenska pass håller en hög säkerhetsnivå. De är svåra att förfalska. Det är också svårt att använda en annan persons pass, eftersom den ansiktsbild och de fingeravtryck som tas vid en passkontroll kan jämföras biometriskt med den ansiktsbild och de fingeravtryck som finns sparade i passet. Det går därigenom att upptäcka om en person försöker använda någon annans pass, även om personerna är lika.

Ett problem som däremot är svårt att motverka effektivt med dagens regelverk är den typ av identitetsstöld som går ut på att en person utger sig för att vara någon annan redan när han eller hon ansöker om pass. Det händer således att en person lyckas få pass under felaktig identitet eller att en och samma person lyckas få flera pass under olika identiteter. Sådana pass kan användas för brottslig verksamhet. Identitetsstölden går inte heller att upptäcka vid en passkontroll, eftersom den ansiktsbild och de fingeravtryck som finnas sparade i passet faktiskt tillhör den som använder passet.

Sökandens identitet ska naturligtvis kontrolleras när han eller hon ansöker om pass. Identiteten kan dock styrkas på olika sätt och ytterst kan det räcka att t.ex. en anhörig intygar att sökanden är den som han eller hon utger sig för att vara. Det finns alltid en risk för att sökanden identifierar sig med en förfalskad identitetshandling eller ett felaktigt intyg. I dessa fall hjälper det inte att passet i sig håller en hög säkerhetsnivå, eftersom det kommer att utfärdas för en person som inte är den som han eller hon utger sig för att vara.

Detta problem har genom åren uppmärksammats av flera olika myndigheter. Polismyndigheten och dåvarande Rikspolisstyrelsen har pekat på behovet av att biometriskt kunna jämföra det senast tagna fotografiet med övriga bilder i passregistret för att säkerställa sökandens identitet. Statens kriminaltekniska laboratorium, numera Nationellt forensiskt centrum inom Polismyndigheten, har i ett yttrande över promemorian Fingeravtryck i pass (Ju2008/7893/PO) framfört att problemet är välkänt och att det är en mycket stor brist att det inte finns möjlighet att kontrollera om en person ansöker om pass under flera olika identiteter. Migrationsverket har i ett yttrande över samma promemoria framfört att dagens förbud mot att lagra de biometriska uppgifter som kan tas fram ur ansiktsbilderna är en uppenbar säkerhetsbrist. Genom att tillåta biometriska jämförelser av ansiktsbilder skulle det enligt Migrationsverket bli mycket svårt att få pass under olika identiteter, något som enligt verket är fullt möjligt om den biometriska informationen lagras endast i passet.

Frågan om vilken betydelse missbruk av identitetshandlingar har när det gäller bedrägerier har utretts av 2017 års ID-kortsutredning. I betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14) anger utredningen att antalet anmälda bedrägerier har ökat med 141 procent mellan 2009 och 2018. Under 2018 anmäldes över 250 000 bedrägerier. Enligt en rapport från Brottsförebyggande rådet, som utredningen hänvisar till, ingår någon form av identitetsmissbruk i mer än tre femtedelar av alla anmälda bedrägerier. Enligt rapporten finns det indikationer på att användningen av stulna och falska identiteter ökar och att det inte sällan har kopplingar till organiserad brottslighet. En form av identitetsmissbruk är att en person lyckas skaffa en identitetshandling under falsk identitet.

Felaktigt utfärdade identitetshandlingar, däribland pass, har alltså stor betydelse när det handlar om bedrägeribrottslighet. Felaktigt utfärdade pass kan också användas vid allvarigare brottslighet, som

exempelvis människosmuggling, människohandel och terroristbrott (jfr prop. 2004/05:119 s. 19 och prop. 2008/09:132 s. 6).

Biometriska jämförelser av ansiktsbilder bör tillåtas

Ett pass är en betydelsefull handling och det ska gå att lita på att de identitetsuppgifter som anges i ett pass stämmer. Pass som utfärdas på felaktiga grunder kan som framgått användas i brottsligt syfte.

Den som ansöker om pass är skyldig att styrka sin identitet på ett tillförlitligt sätt i samband med ansökan. Detta framgår av passlagen och passförordningen. Enligt förvaltningslagen ska en myndighet se till att ett ärende blir utrett i den omfattning som dess beskaffenhet kräver. Starka skäl talar för att passmyndigheterna som ett moment i handläggningen ska ha möjlighet att söka i passregistret med hjälp av den ansiktsbild som tas. Som Polismyndigheten påpekar skulle det vara ett effektivt verktyg för att säkerställa sökandens identitet.

Sådana sökningar innebär samtidigt att känsliga personuppgifter i form av biometriska uppgifter behandlas. Det är inte självklart att sökningen är absolut nödvändig för passhandläggningen och det är därför inte givet att sökningen kan ske med stöd av de regler som har föreslagits i fråga om känsliga personuppgifter i allmänhet. Särskilda bestämmelser som möjliggör biometriska jämförelser av ansiktsbilder i samband med en passansökan bör därför övervägas.

För att biometriska uppgifter ska få behandlas med stöd av artikel 9.2 g i dataskyddsförordningen krävs som framgått att behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, att den står i proportion till det syfte som eftersträvas och att den omfattas av regler som skyddar den registrerades rättigheter och intressen.

Att motverka missbruk av pass och säkerställa att pass utfärdas för rätt person, i enlighet med passlagstiftningen, utgör ett sådant viktigt allmänt intresse som avses i artikel 9.2 g. Möjligheten att söka i passregistret med hjälp av den ansiktsbild som tas vid ansökan är nödvändig för att säkerställa att pass utfärdas för rätt person. Hur begreppet nödvändig ska tolkas har berörts tidigare (avsnitt 6.6.2). Sökmöjligheten är ett effektivt verktyg mot identitetsmissbruk och risken för integritetsintrång framstår som begränsad. En kontroll av det aktuella slaget skyddar enskilda mot identitetskapning och risken för identitetskapning måste för de allra flesta människor

framstå som ett större hot mot den personliga integriteten än att vissa myndigheter får jämföra ansiktsbilder under reglerade former. Det är inte heller fråga om att någon ny kategori av personuppgifter samlas in. Ansiktsbilderna och de biometriska uppgifter som kan tas fram ur dessa behandlas redan i passverksamheten. Det är bara möjligheten till sökning som förändras. Som utvecklas nedan står vidare klart att en biometrisk jämförelse av ansiktsbilder kommer att förenas med sådana skyddsåtgärder som avses i artikel 9.2 g.

Slutsatsen är alltså att biometriska jämförelser av ansiktsbilder, i syfte att kontrollera sökandens identitet och innehav av pass vid en ansökan om pass, är tillåtna enligt dataskyddsförordningen.

Passdatalagen bör därmed tillåta att den ansiktsbild som tas vid en passansökan jämförs biometriskt med bilderna i passregistret. För att möjliggöra det bör passregistret få innehålla både ansiktsbilder och biometriska uppgifter som har tagits fram ur ansiktsbilder. De biometriska uppgifterna kan därmed sparas självständigt eller som en del av ansiktsbilderna, genom att dessa sparas i ett sådant tekniskt format att biometriska jämförelser kan göras. Dagens bestämmelse om att de biometriska uppgifter som tas fram ur ansiktsbilder ska förstöras när ett passärende avslutas bör upphävas. Dagens förbud mot sökning bör justeras så att ansiktsbilden och de biometriska uppgifter som tas fram ur ansiktsbilden får användas vid sökning i passregistret för att kontrollera sökandens identitet och innehav av pass i samband med en passansökan. Sökningar för andra ändamål bör däremot vara förbjudna även i fortsättningen, för att värna den registrerades integritet så långt som möjligt (jfr avsnitt 6.11).

När det gäller fingeravtrycken och de biometriska uppgifter som tas fram ur dessa föreslås inga förändringar jämfört med dagens regelverk. Dessa uppgifter ska även i fortsättningen förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits (jfr avsnitt 6.14). Fingeravtrycken ska inte heller få användas vid sökning. Det har inte kommit fram att det finns något behov av att kunna behandla fingeravtryck på nya sätt, som skulle väga upp det integritetsintrång som en utvidgad behandling skulle medföra.

Skyddsåtgärder och sekretess för biometriska uppgifter

I passdatalagen föreslås ett flertal bestämmelser som syftar till att säkerställa den registrerades rättigheter och intressen. De reglerna kommer att gälla även när biometriska uppgifter behandlas. I avsnitt 6.5 lämnas förslag som klargör hur ansvaret för behandlingen av personuppgifter i passverksamheten är fördelat mellan de olika myndigheterna. Genom de ändamålsbestämmelser som föreslås i avsnitt 6.6 klargörs det när personuppgifter över huvud taget får behandlas. Bortsett från rätten att göra invändningar mot tillåten behandling föreslås det i avsnitt 6.7 att den registrerades rättigheter enligt dataskyddsförordningen ska gälla när personuppgifter behandlas i passverksamheten. I avsnitt 6.8 föreslås att den interna tillgången till personuppgifter inom myndigheterna ska begränsas.

I avsnitt 6.9 föreslås bestämmelser som uttömmande anger vad passregistret och passtillståndsregistret får innehålla och i avsnitt 6.11 föreslås flera sökförbud och sök begränsningar. Möjligheten att lämna ut personuppgifter elektroniskt ska enligt förslagen i avsnitt 6.12 vara begränsad och i avsnitt 6.14 finns förslag om hur länge biometriska uppgifter och andra uppgifter får bevaras i passregistret.

Eftersom biometriska uppgifter utgör känsliga personuppgifter kommer höga säkerhetskrav att gälla vid behandlingen (jfr artikel 32 i dataskyddsförordningen). De personuppgiftsansvariga ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder.

Utöver detta kommer behandlingen av biometriska uppgifter att omfattas av dataskyddslagens bestämmelser om tillsyn, skadestånd och överklagande. Detta behandlas närmare i avsnitt 6.15.

Vid sidan av dessa skyddsåtgärder bör det även säkerställas att de biometriska uppgifter som behandlas har ett adekvat sekretesskydd. Sekretessen för biometriska uppgifter behandlas i avsnitt 7.

Sammantaget kommer det därmed att finnas bestämmelser som skyddar den registrerades grundläggande rättigheter och intressen i den mening som avses i artikel 9.2 g i dataskyddsförordningen.

Vad händer om sökningen leder till en träff?

En viktig fråga är vad som händer om den biometriska jämförelsen resulterar i en träff, dvs. om datorsystemet anger att sökanden redan har pass under en annan identitet eller att den nytagna bilden inte

stämmer överens med de bilder som finns i sökandens tidigare ärenden. Kan man lita på tekniken eller kan träffen vara felaktig?

Ett beslut om att utfärda ett pass, att avslå en passansökan eller att återkalla ett pass ska fattas efter en prövning av omständigheterna i det enskilda fallet. En träff i passregistret är därför i första hand en signal om att sökandens identitet behöver utredas ytterligare. Om det visar sig att sökanden inte kan anses ha styrkt sin identitet finns det dock stöd i passlagen för att avslå passansökan (7 § 1 passlagen) eller återkalla ett tidigare utfärdat pass (12 § första stycket 8 samma lag). Ett sådant beslut ska motiveras och kan överklagas till allmän förvaltningsdomstol. Det finns alltså rättssäkerhetsgarantier.

Övriga frågor om biometriska uppgifter

Det förslag som nu lämnas innebär att biometriska uppgifter som tas fram ur ansiktsbilder får sparas i passregistret. Syftet med det är att möjliggöra sökning i passregistret med hjälp av den ansiktsbild som tas vid en passansökan. De biometriska uppgifterna kommer dock att omfattas av samtliga ändamålsbestämmelser som har föreslagits i avsnitt 6.6. Det betyder att exempelvis Polismyndigheten i vissa fall kommer att ha möjlighet att behandla uppgifterna bl.a. för att bekämpa brott. Detta kan framstå som långtgående men i praktiken är integritetsriskerna begränsade. Polismyndigheten har redan i dag tillgång till ansiktsbilderna. De biometriska uppgifterna fyller en funktion framför allt när det handlar om möjligheten att utföra sökningar med hjälp av bilderna. Den möjligheten kommer att vara starkt begränsad (jfr avsnitt 6.11). När Polismyndigheten bekämpar brott gäller vidare att biometriska uppgifter får behandlas bara om det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 4 § polisens brottsdatalog). De biometriska uppgifterna kommer slutligen, som framgått, att omfattas av övriga skyddsbestämmelser i passdatalagen och av sekretess i enlighet med förslaget i avsnitt 7.

En särskild fråga är om den ansiktsbild som tas i samband med en ansökan om pass bör få jämföras biometriskt även med de bilder som finns i registret över nationella identitetskort. En sådan möjlighet skulle förbättra kontrollen av sökandens identitet ytterligare och motverka att en och samma person får pass och nationellt identitetskort under olika identiteter. Som angetts i avsnitt 2 har 2017 års ID-

kortsutredning emellertid föreslagit att förordningen om nationellt identitetskort ska upphävas och ersättas av ett regelverk om statliga identitetskort. I nuläget finns det därför inte skäl att föreslå någon möjlighet till sökning i registret över nationella identitetskort. Om utredningens förslag genomförs talar däremot starka skäl för att den ansiktsbild som tas i samband en passansökan bör kunna jämföras tekniskt även med bilderna i registret över statliga identitetskort.

Det ska slutligen sägas att begreppet biometriska data, som i dag används i passlagen, bör utmönstras. Biometriska uppgifter är det begrepp som används i dataskyddsförordningen och någon skillnad mellan uttrycken finns inte. Begreppet biometriska uppgifter bör mot den bakgrunden användas i både passlagen och passdatalagen.

6.10.5 Lagöverträdelser och personnummer

Bedömning: Bortsett från en sökbegränsning behöver lagen inte innehålla några bestämmelser om hur personuppgifter som rör lagöverträdelser får behandlas. Lagen behöver inte innehålla några bestämmelser om personnummer eller samordningsnummer.

Den tidigare promemorians bedömning överensstämmer med bedömningen här.

Remissinstanserna tillstyrker eller har inga invändningar mot bedömningen.

Skälen för bedömningen

Uppgifter om lagöverträdelser

Uppgifter om lagöverträdelser är inte känsliga personuppgifter men anses ändå vara en typ av uppgifter som förtjänar ett särskilt skydd.

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder får enligt artikel 10 i dataskyddsförordningen endast utföras under kontroll av en myndighet eller då sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

Ett fullständigt register över fällande domar i brottmål får enligt samma artikel endast föras under kontroll av en myndighet.

I 3 kap. 8 § dataskyddslagen anges att personuppgifter som avses i artikel 10 i dataskyddsförordning får behandlas av myndigheter.

I passverksamheten behandlas uppgifter om lagöverträdelser och straffprocessuella tvångsmedel som t.ex. häktning. Uppgifterna är nödvändiga att behandla eftersom bl.a. häktning och fängelsestraff kan medföra att en passansökan ska avslås enligt 7 § passlagen eller att ett pass ska återkallas enligt 10 § samma lag. Eftersom uppgifter av detta slag får behandlas av myndigheter behövs det inte något uttryckligt stöd i passdatalagen för att behandlingen ska kunna ske.

I nästa avsnitt föreslås ett förbud mot sökningar som syftar till att få fram ett urval av personer grundat på personuppgifter som rör lagöverträdelser. Bortsett från det förbudet finns det inte skäl att inskränka myndigheternas möjlighet att behandla uppgifter som rör lagöverträdelser, utöver vad som följer av ändamålsbestämmelserna och övriga tillämpliga bestämmelser.

Uppgifter om person- och samordningsnummer

Personnummer och samordningsnummer är inte heller känsliga personuppgifter i dataskyddsförordningens mening. De har ändå en särställning genom att medlemsstaterna har getts en möjlighet att införa särskilda villkor för behandlingen (artikel 87 i förordningen).

Av 3 kap. 10 § dataskyddslagen framgår att personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

I passverksamheten behandlas person- och samordningsnummer i stor utsträckning. Vikten av en säker identifiering är uppenbar. Någon uttrycklig bestämmelse som ger myndigheterna stöd för att behandla dessa person- och samordningsnummer behövs därför inte. Det finns inte heller skäl att inskränka myndigheternas möjlighet att behandla dessa uppgifter, utöver vad som följer av 3 kap. 10 § dataskyddslagen och övriga tillämpliga bestämmelser.

6.11 Sökbegränsningar i verksamheten

Förslag: Det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller personuppgifter som rör lagöverträdelser.

Det ska också vara förbjudet att använda fingeravtryck och ansiktsbilder samt biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder som sökbegrepp. Trots förbudet ska den ansiktsbild som tas i samband med en passansökan, och de biometriska uppgifter som tas fram ur den ansiktsbilden, få användas vid sökning i passregistret för att kontrollera sökandens identitet och innehav av pass.

De förbud som har angetts ovan ska gälla även vid sökningar i passregistret och passtillståndsregistret för andra ändamål än handläggning av ärenden om pass.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. I promemorian föreslås att uppgifter som avslöjar ras eller etniskt ursprung, uppgifter som rör hälsa samt uppgifter om lagöverträdelser inte ska få användas som sökbegrepp. Övriga typer av känsliga personuppgifter berörs inte. Det föreslås vidare att de fingeravtryck och den ansiktsbild som tas vid en passansökan, samt de biometriska data som kan tas fram ur dessa, inte ska få användas vid sökning med hjälp av automatiserad behandling.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Polismyndigheten* påpekar dock, som nämnts i förra avsnittet, att det föreslagna sökförbudet hindrar biometriska jämförelser av ansiktsbilder i samband med ansökningar om pass. *Kammarrätten i Göteborg* ifrågasätter om det är nödvändigt att ange att sökförbudet i fråga om fingeravtryck och ansiktsbilder gäller vid sökning med hjälp av automatiserad behandling. Enligt kammarrätten följer avgränsningen till automatiserad behandling redan av bestämmelserna om lagens tillämpningsområde.

Skälen för förslaget

Allmänt om sökbegränsningar

Modern informationsteknik medför att stora mängder information enkelt kan lagras och att informationen kan göras tillgänglig för olika sökningar och sammanställningar. För myndigheternas del bidrar detta i hög grad till en effektiv verksamhet. För den registrerade kan det samtidigt medföra en särskild risk för integritetsintrång. Det gäller i synnerhet sökningar som rör känsliga personuppgifter.

Sökning och sammanställning av personuppgifter på elektronisk väg är en sådan behandling som omfattas av dataskyddsförordningen och som kommer att omfattas av passdatalagen. Ett skydd för den personliga integriteten finns genom de allmänna bestämmelserna i dataskyddsförordningen och de bestämmelser som föreslås i denna promemoria. Möjligheten att söka bland personuppgifter kommer således att begränsas genom de bestämmelser som föreslås om bl.a. tillåtna ändamål, passregistrets innehåll och säkerhetsåtgärder.

För att ytterligare värna den registrerades personliga integritet bör särskilda bestämmelser om sökförbud eller sökbegränsningar ändå övervägas. Sökbegränsningar är en skyddsåtgärd som finns i många registerförfattningar och dataskyddsförordningen hindrar inte att skyddsåtgärder av det slaget införs genom nationell rätt.

Nedan föreslås att två typer av sökbegränsningar ska gälla enligt passdatalagen. Det handlar dels om ett förbud mot sökningar i visst syfte, dels om ett förbud mot vissa sökbegrepp. Som *Kammarrätten i Göteborg* påpekar behöver det inte anges att begränsningarna gäller vid sökning med hjälp av automatiserad behandling. Bestämmelserna bör ha samma tillämpningsområde som passdatalagen i övrigt.

Ett allmänt förbud mot sökningar i visst syfte

I flera registerförfattningar finns begränsningar som innebär att det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. En sådan begränsning gäller också när känsliga personuppgifter behandlas med stöd av 3 kap. 3 § dataskyddslagen. När den begränsningen infördes angavs det att en sökning som avslöjar och sammanställer känsliga personuppgifter är en åtgärd som i sig innebär en integritetskränkning.

Företeelsen ansågs ligga nära det som ursprungligen har motiverat förbudet mot behandling av känsliga personuppgifter, nämligen möjligheten att kartlägga personer på grundval av t.ex. etnicitet eller politiska åsikter. Med en sökbegränsning uppnås därmed ett skydd av de intressen som ska värnas genom det principiella förbudet mot behandling av känsliga personuppgifter (prop. 2017/18:105 s. 90).

Sökbegränsningen i dataskyddslagen är, liksom motsvarande sökbegränsningar i andra registerförfattningar, inte absolut. Den förbjuder visserligen alla former av sökningar som görs för att få fram ett urval av personer som exempelvis har en viss politisk åsikt, religiös åskådning eller sexuell läggning. Den hindrar däremot inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, exempelvis för att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård (prop. 2017/18:105 s. 195).

Sökbegränsningen enligt dataskyddslagen gäller bara när känsliga personuppgifter behandlas med stöd av 3 kap. 3 § första stycket dataskyddslagen. Den gäller alltså inte när känsliga personuppgifter behandlas med stöd av bestämmelser i en annan författning. I denna promemoria föreslås särskilda bestämmelser som anger när känsliga personuppgifter får behandlas. Den sökbegränsning som framgår av dataskyddslagen kommer därför inte att vara tillämplig när känsliga personuppgifter behandlas i passverksamheten. En bestämmelse av samma innebörd, som förbjuder sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter, bör därför införas i passdatalagen. Det klargörs därmed att sökningar som görs för att få fram ett urval av personer som har exempelvis ett visst etniskt ursprung inte är tillåtna.

Den angivna sökbegränsningen bör gälla även i fråga om sådana personuppgifter som avses i artikel 10 i dataskyddsförordningen, dvs. uppgifter om lagöverträdelse och straffprocessuella tvångsmedel. Sådana uppgifter är integritetskänsliga, även om de inte utgör känsliga personuppgifter i dataskyddsförordningens mening.

Ett kompletterande förbud mot vissa sökbegrepp

I dag gäller att de fingeravtryck och den ansiktsbild som tas vid en passansökan inte får användas vid sökning. Samma sak gäller i fråga om de biometriska data som kan tas fram ur fingeravtrycken och

ansiktsbilden. Förbudet framgår av 6 b § passlagen och är absolut. Det saknar alltså betydelse vilket syfte en sådan sökning har.

Eftersom sökförbudet är absolut får myndigheterna inte utföra en sökning med ett förbudet sökbegrepp ens för att tillmötesgå en begäran om utlämnande av allmän handling. Detta följer av 2 kap. 7 § tryckfrihetsförordningen. En sammanställning anses enligt den paragrafen över huvud taget inte förvarad hos myndigheten, om den innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig.

För att skydda den registrerades personliga integritet bör det absoluta förbudet mot användning av fingeravtryck och ansiktsbilder som sökbegrepp i princip behållas. Förbudet bör dock föras över från passlagen till passdatalagen och justeras i två avseenden.

För det första bör förbudet utvidgas så att det inte bara träffar de fingeravtryck och den ansiktsbild som tas vid en passansökan. Det bör vara förbudet att över huvud taget använda fingeravtryck och ansiktsbilder, inklusive biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder, vid sökning i passverksamheten. Det kan annars framstå som tillåtet att utföra sökningar med hjälp av fingeravtryck eller ansiktsbilder som har tagits i något annat sammanhang. Sökförbudet bör alltså utformas så att det tydligt framgår att fingeravtryck och ansiktsbilder inte får användas som sökbegrepp oavsett om dessa har tagits vid en passansökan eller i något annat sammanhang. Förbudet bör även gälla biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder.

För det andra bör sökförbudet utformas så att det inte hindrar den biometriska jämförelse av ansiktsbilder som har beskrivits i avsnitt 6.10.4. Genom undantag från sökförbudet bör det alltså vara tillåtet att använda den ansiktsbild som tas vid en passansökan, och de biometriska uppgifter som tas fram ur ansiktsbilden, vid sökning i passregistret för att kontrollera sökandens identitet och innehav av pass i samband med en ansökan om pass. Detta bör dock vara det enda undantaget från det i övrigt heltäckande sökförbudet.

Sökförbud utanför själva passverksamheten

En särskild fråga är om sökförbudena ovan bör gälla bara när personuppgifter behandlas i passverksamheten eller om förbudena bör gälla

även när exempelvis Polismyndigheten behandlar personuppgifter i passverksamheten för andra ändamål, som t.ex. brottsbekämpning.

Som registerförande myndighet har Polismyndigheten en direkt tillgång till både passregistret och passtillståndsregistret. Genom de bestämmelser om direktåtkomst som föreslås i avsnitt 6.12.2 kan även andra passmyndigheter och Utrikesdepartementet komma att ha tillgång till dessa register. De sekundära ändamålsbestämmelser som har föreslagits i avsnitt 6.6 tillåter att passmyndigheterna och Utrikesdepartementet använder personuppgifterna i passregistret och passtillståndsregistret för andra ändamål än passhandläggning. För Polismyndighetens del handlar det bl.a. om gränskontroll och brottsbekämpning. Vid behandling för sekundära ändamål vid sidan av själva passverksamheten kommer passdatalagen inte att gälla. Sådan behandling kan i stället omfattas av t.ex. utlänningsdatalagen, brottsdatalagen, polisens brottsdatalag eller någon annan reglering.

Med hänsyn till den registrerades personliga integritet bör lagens sökförbud gälla även när personuppgifter behandlas för sekundära ändamål. Det bör därför införas en bestämmelse i lagen som klargör att sökförbuden gäller även vid sökningar i passregistret och passtillståndsregistret för andra ändamål än handläggning av ärenden om pass. Det tydliggörs därmed att t.ex. ansiktsbilder inte får användas vid sökningar i passregistret eller passtillståndsregistret vare sig inom ramen för passhandläggning eller inom ramen för t.ex. gränskontroll eller brottsbekämpning.

6.12 Elektroniskt utlämnande av personuppgifter

6.12.1 Elektroniskt utlämnande i allmänhet

Förslag: Personuppgifter ska få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. I promemorian föreslås att personuppgifter ska få lämnas ut på detta sätt utan någon lämplighetsprövning.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Sveriges advokatsamfund* anser dock att ett automatiserat förfarande för utlämnande kan medföra

att gränserna suddas ut mellan utlämnande på medium för automatiserad behandling och direktåtkomst, vilket kan vara en fara för den personliga integriteten. Enligt advokatsamfundet aktualiseras också behovet av kryptering av personuppgifterna för att undvika obehörig åtkomst, särskilt beträffande känsliga personuppgifter.

Skälen för förslaget: Utlämnande av personuppgifter utgör en sådan behandling som omfattas av dataskyddsförordningen och den föreslagna passdatalagen. Utlämnande av personuppgifter kan ske antingen i fysisk form, t.ex. genom att ett papper lämnas ut, eller i elektronisk form. När det gäller elektroniskt utlämnande skiljer man mellan direktåtkomst och annat elektroniskt utlämnande.

För annat elektroniskt utlämnande än genom direktåtkomst har begreppet ”utlämnande på medium för automatiserad behandling” ofta använts. Ett sådant utlämnande kan göras t.ex. genom att information förs över via e-post, lämnas ut på ett usb-minne eller förs över från ett datorsystem till ett annat. Informationshanteringsutredningen har kritiserat begreppet och föreslagit att uttrycket ”utlämnande i elektronisk form” ska användas för alla elektroniska utlämnanden som inte utgör direktåtkomst (betänkandet Myndighetsdatalag, SOU 2015:39 s. 442 f.). Det nya begreppet används i flera registerförfattningar och bör användas även i passdatalagen.

Dataskyddsförordningen innehåller inga särskilda bestämmelser som begränsar möjligheten till elektroniskt utlämnande. Ett sådant utlämnande är tillåtet förutsatt att det sker i enlighet med de ändamål som är bestämda för personuppgiftsbehandlingen i stort, att kraven på informationssäkerhet upprätthålls och att förordningens regler följs i övrigt. Dataskyddsförordningen medför samtidigt inte några hinder mot nationella bestämmelser som begränsar möjligheten till elektroniskt utlämnande (jfr prop. 2017/18:113 s. 12).

När ett utlämnande är tillåtet talar starka effektivitetsskäl för att passmyndigheterna och Utrikesdepartementet ska kunna lämna ut personuppgifter elektroniskt. Om ett sådant utlämnande inte får ske måste den utlämnande myndigheten göra utskrifter på papper och skicka dessa till mottagaren. Mottagaren kan därefter behöva överföra uppgifterna till elektronisk form igen för att kunna använda dem. En sådan ordning framstår som ineffektiv och otidsenlig.

Utlämnande av personuppgifter på elektronisk väg kan dock, som *Sveriges advokatsamfund* påpekar, innebära vissa risker från integritetssynpunkt. Ett sådant utlämnande medför att mottagaren

kan bearbeta informationen och sammanställa den med uppgifter från andra källor. Samtidigt ska skillnaden mellan ett elektroniskt utlämnande och ett utlämnande på papper inte överdrivas. Text på ett papper går enkelt att omvandla till elektroniska uppgifter. Ett skydd för den personliga integriteten finns dessutom genom de ändamålsbestämmelser som föreslås, som sätter vissa gränser för när ett elektroniskt utlämnande alls kan ske, och de säkerhetskrav som framgår direkt av dataskyddsförordningen.

Elektroniskt utlämnande i annan form än genom direktåtkomst bör mot denna bakgrund tillåtas. Det finns emellertid skäl att stärka integritetsskyddet något i jämförelse med vad som föreslås i den tidigare promemorian. Passregistret innehåller uppgifter om ett stort antal människor och uppgifterna är normalt sett offentliga. Det medför att förhållandevis många uppgifter kan komma att lämnas ut elektroniskt, till både myndigheter och enskilda. De särskilda sekretessbestämmelser som gäller för fotografier i passregistret (avsnitt 3.4.4) och för uppgifter som efter ett utlämnande kan antas komma att behandlas i strid med dataskyddsregleringen (21 kap. 7 § offentlighets- och sekretesslagen) undanröjer inte helt de risker som kan uppstå för den personliga integriteten. Det framstår mot den bakgrunden som en god ordning att personuppgifter ska få lämnas ut på elektronisk väg bara efter en särskild lämplighetsprövning.

Det bör således införas en bestämmelse i passdatalagen som anger att passmyndigheterna och Utrikesdepartementet får lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om detta inte är olämpligt. Motsvarande bestämmelser finns i bl.a. domstolsdatalagen och polisens brottsdatalag. Vid den prövning som ska göras har det betydelse vem mottagaren är – en myndighet eller en enskild – och om det på grund av personuppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet i förlängningen kan leda till integritetsrisker. Om ett elektroniskt utlämnande bedöms vara olämpligt får personuppgifterna i stället lämnas ut på papper.

6.12.2 Elektroniskt utlämnande genom direktåtkomst

Förslag: Personuppgifter ska få lämnas ut elektroniskt genom direktåtkomst endast i följande fall och på följande villkor:

- Uppgift om en passhandlings giltighet ska få lämnas ut genom direktåtkomst oavsett vem mottagaren är.
- Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) ska få medge varandra direktåtkomst till personuppgifter. Åtkomsten ska begränsas till de personuppgifter som varje myndighet behöver för att handlägga passärenden.
- Säkerhetspolisen ska få medges direktåtkomst till personuppgifter i passregistret. Åtkomsten ska begränsas till de personuppgifter som Säkerhetspolisen behöver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Samma sökförbud ska gälla för Säkerhetspolisen som för Polismyndigheten.

Den tidigare promemorian innehåller inget förslag i frågan.

Remissinstanserna: Nästan ingen av remissinstanserna yttrar sig särskilt i frågan. *Polismyndigheten* framför dock att lagförslaget bör kompletteras med en bestämmelse om ömsesidig direktåtkomst mellan passmyndigheterna. Enligt Polismyndigheten behöver andra passmyndigheter ha åtkomst till uppgifterna i Polismyndighetens passverksamhet för att kunna bedriva sin egen passverksamhet. Polismyndigheten anser vidare att passdatalagen bör ge stöd för en webblösning som innebär att myndigheten lämnar ut uppgifter om en passhandlings giltighet. Enligt Polismyndigheten har banker och näringsliv ett behov av att enkelt och snabbt kunna verifiera om ett pass är giltigt. *Säkerhetspolisen* framför att det är av stor vikt för myndigheten att ha direktåtkomst till passregistret och registret över omständigheter som avses i 20 § 1 och 3 passlagen. Enligt Säkerhetspolisen kan det vara direkt avgörande för myndighetens underrättelse- och utredningsarbete att medarbetarna omedelbart, säkert och självständigt kan ta del av dessa registeruppgifter. Att Säkerhetspolisen ska begära ut uppgifterna i varje enskilt fall är inte ett effektivt arbetssätt, oaktat att de kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst.

Skälen för förslaget

Vad är direktåtkomst?

Det finns ingen legaldefinition av begreppet direktåtkomst. Det som vanligtvis avses är att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen.

Enligt Informationshanteringsutredningen bör direktåtkomst anses föreligga om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i nuvarande 2 kap. 6 § tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt (SOU 2015:39 s. 390). I avgörandet HFD 2015 ref. 61, som avsåg elektroniskt utlämnande av uppgifter mellan myndigheter, definierade Högsta förvaltningsdomstolen begreppet på samma sätt som Informationshanteringsutredningen.

I begreppet direktåtkomst ligger även att den som ansvarar för registret eller databasen saknar kontroll över vilka uppgifter som mottagaren, dvs. den som har direktåtkomst, tar del av vid ett visst tillfälle. Beslutet om överföring fattas av mottagaren och inte av den som ansvarar för registret eller databasen. Från integritetssynpunkt har det därför ansetts viktigt att frågan om tillgång till uppgifter genom direktåtkomst regleras i särskilda registerförfattningar.

Vilka är riskerna med direktåtkomst?

Elektroniskt utlämnande genom direktåtkomst brukar förknippas med särskilda risker för den personliga integriteten. En sådan risk är att personuppgifterna sprids som en följd av att de upptagningar som direktåtkomsten avser blir allmänna handlingar hos den mottagande myndigheten. Sammanställningar av uppgifter som i samband med direktåtkomst görs tillgängliga för den mottagande myndigheten anses enligt 2 kap. 6 § tryckfrihetsförordningen förvarade hos den mottagande myndigheten och utgör således allmänna handlingar där.

Ju fler myndigheter som har direktåtkomst till uppgifter i ett datasystem, desto större blir alltså allmänhetens möjlighet att få tillgång till uppgifterna. Direktåtkomst innebär typiskt sett också att

personuppgifter blir tillgängliga för fler personer i de verksamheter som har direktåtkomst och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar.

Att en myndighet får tillgång till uppgifter genom direktåtkomst ger dock inte myndigheten rätt att behandla personuppgifterna. Den mottagande myndigheten måste ha ett eget rättsligt stöd för att få behandla uppgifterna. Den mottagande myndigheten måste också i övrigt uppfylla de skyldigheter som är förenade med behandlingen.

För att minska riskerna med elektroniskt utlämnande genom direktåtkomst har vissa sekretessbestämmelser införts. I 11 kap. 4 § offentlighets- och sekretesslagen anges att om en myndighet har elektronisk tillgång till en upptagning för automatiserad behandling hos en annan myndighet, och en uppgift i denna upptagning är sekretessreglerad, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten. Sekretess för personuppgifter gäller vidare enligt 21 kap. 7 § offentlighets- och sekretesslagen om det kan antas att ett utlämnande skulle medföra att uppgifterna behandlas i strid med dataskyddsförordningen eller dataskyddslagen.

Direktåtkomst bör tillåtas i vissa angivna fall

Direktåtkomst kan innebära effektivitetsvinster för den myndighet som behöver uppgifter från en annan myndighet i sin verksamhet. Genom direktåtkomst behöver myndigheten inte vända sig till den utlämnande myndigheten med en särskild begäran. Tjänstemännen kan i stället själva eftersöka och hämta den information som behövs.

Även för en enskild som vill ta del av uppgifter som finns hos en myndighet kan direktåtkomst innebära fördelar. Han eller hon får tillgång till uppgifterna direkt utan att behöva vänta på svar.

Direktåtkomst kan också innebära fördelar för den utlämnande myndigheten, som inte behöver avsätta resurser för att hantera olika förfrågningar om utlämnande. Det finns också fördelar från ett informationssäkerhetsperspektiv, eftersom överföring ofta kan ske på ett säkrare sätt genom direktåtkomst än genom t.ex. e-post.

Mot denna bakgrund bör personuppgifter i passverksamheten kunna lämnas ut genom direktåtkomst i vissa fall. Det bör samtidigt påpekas att uppgifter ofta kan lämnas ut elektroniskt på ett effektivt sätt utan att det är fråga om direktåtkomst i rättslig mening. Det går

t.ex. att utforma datorsystem som innebär att en myndighet lämnar ut uppgifter mer eller mindre automatiskt utan att det är fråga om direktåtkomst (jfr det ovan nämnda avgörandet HFD 2015 ref. 61). Utlämnande genom direktåtkomst är alltså inte nödvändigtvis mer effektivt än andra former av elektroniskt utlämnande. Som framgått kan direktåtkomst dessutom innebära särskilda integritetsrisker.

Sammanfattningsvis bör personuppgifter i passverksamheten kunna lämnas ut genom direktåtkomst bara i vissa tydligt avgränsade fall. Nedan föreslås att uppgifter om ett pass giltighet bör kunna lämnas ut på detta sätt. Vidare föreslås att passmyndigheterna och Utrikesdepartementet bör kunna medge varandra direktåtkomst. Slutligen föreslås att Säkerhetspolisen i viss uträkning bör kunna medges direktåtkomst. Med hänsyn till den registrerades personliga integritet bör direktåtkomst inte kunna medges i några andra fall.

För att möjliggöra direktåtkomst behövs vissa sekretessbrytande bestämmelser. Hur dessa bör utformas behandlas i nästa avsnitt.

Direktåtkomst till uppgifter om passhandlingars giltighet

Pass används i relativt stor utsträckning som identitetshandlingar. Det finns därför ett intresse av ett enkelt och väl fungerande system för att kontrollera om ett pass är giltigt eller inte. Uppgiften att ett visst pass är giltigt eller inte giltigt bör betraktas som en personuppgift, om informationen kan hänföras till en viss individ. Ett utlämnande utgör i dessa fall en behandling av personuppgifter.

Uppgiften att ett visst pass är giltigt eller inte giltigt måste anses vara offentlig (jfr avsnitt 3.4.4). Det är därmed fråga om en uppgift som normalt sett ska lämnas ut, om det begärs. Frågan är om det bör införas en bestämmelse som ger uttryckligt stöd för ett utlämnande genom direktåtkomst. En sådan bestämmelse skulle ge ett tydligt stöd för den typ av webblösning som *Polismyndigheten* nämner, dvs. en webbaserad tjänst där t.ex. en bank eller butik på egen hand kan kontrollera om det pass som en person visar upp är giltigt. En sådan tjänst kan naturligtvis också användas av passinnehavaren själv, om han eller hon av någon anledning vill kontrollera passets status.

Det kan konstateras att motsvarande fråga är reglerad i lagen (2015:899) om identitetskort för folkbokförda i Sverige. Enligt den lagen kan en person som har fyllt 13 år och är folkbokförd i landet

efter ansökan få ett identitetskort utfärdat av Skatteverket. Uppgift om ett sådant identitetskorts giltighet får enligt 16 § i lagen lämnas ut genom direktåtkomst. Enligt förarbetena är direktåtkomsten inte av särskilt integritetskänslig karaktär, eftersom den är begränsad till uppgiften om identitetskortets giltighet (prop. 2015/16:28 s. 64).

Det framstår som rimligt att uppgifter om passhandlingars giltighet ska kunna lämnas ut genom direktåtkomst på samma sätt som när det gäller identitetskort för folkbokförda. Detta förenklar för den som vill veta om ett visst pass är giltigt, samtidigt som den information som kan lämnas ut genom direktåtkomsten är mycket begränsad. En bestämmelse som ger tydligt stöd för direktåtkomst till uppgifter om passhandlingars giltighet bör alltså införas i lagen.

Inbördes direktåtkomst för myndigheter som utfärdar pass

Ärenden om pass handläggs av flera myndigheter. Polismyndigheten samt vissa ambassader och konsulat är passmyndigheter. Diplomats- och tjänstepass utfärdas av Utrikesdepartementet. För att kunna handlägga passärenden behöver dessa myndigheter ofta ha tillgång till uppgifter som finns hos någon av de andra myndigheterna. Varje myndighet behöver t.ex. veta om den som ansöker om ett pass redan har ett giltigt pass eller om passtillstånd krävs. Det bör mot den bakgrunden införas uttryckliga bestämmelser som klargör att de angivna myndigheterna får medge varandra direktåtkomst. Som Polismyndigheten är inne på framstår detta som en förutsättning för att passärenden ska kunna handläggas effektivt. Direktåtkomsten bör inte begränsas till uppgifter i passregistret utan kunna avse även uppgifter i passtillståndsregistret samt uppgifter som behandlas i verksamheten i övrigt, t.ex. inom ramen för ett pågående ärende. Även sådana uppgifter behövs för handläggningen av passärenden.

Direktåtkomsten bör dock begränsas till de uppgifter som var och en av myndigheterna behöver för att kunna handlägga ärenden om pass. Den begränsningen kan regleras i passdataförordningen.

Direktåtkomst till passregistret för Säkerhetspolisen

Säkerhetspolisen var länge en del av Rikspolisstyrelsen men är sedan den 1 januari 2015 en självständig myndighet. Till Säkerhetspolisens

huvudsakliga arbetsuppgifter hör enligt 3 § polislagen (1984:387) att förebygga, förhindra, upptäcka, utreda och beivra brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott.

Säkerhetspolisen har förhållandevis goda möjligheter att ta del av uppgifter från passverksamheten enligt gällande rätt. Uppgifter som inte omfattas av sekretess ska på begäran lämnas ut till myndigheten, om det inte hindrar arbetets behöriga gång hos den utlämnande myndigheten (6 kap. 5 § offentlighets- och sekretesslagen). Enligt den sekretessbrytande bestämmelsen i 23 § passförordningen har Polismyndigheten dessutom en skyldighet att på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen. Något uttryckligt stöd för direktåtkomst finns dock inte i dag.

Enligt förslaget i avsnitt 6.6.4 bör Polismyndigheten få behandla personuppgifter som har samlats in för handläggning av passärenden om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Polismyndigheten är en passmyndighet och ansvarar själv för förändret av passregistret. De personuppgifter som finns i passverksamheten är alltså direkt åtkomliga för myndigheten som sådan. Att den interna tillgången till personuppgifter ska vara begränsad är en annan sak. Det framstår som angeläget och naturligt att Säkerhetspolisen, som är den andra av våra två polismyndigheter, har motsvarande tillgång till åtminstone vissa av uppgifterna. Det bör därför införas uttryckliga bestämmelser om direktåtkomst för myndigheten. Säkerhetspolisens behandling av de personuppgifter som myndigheten får tillgång till regleras för närvarande främst i 2010 års polisdata lag. En ny reglering bereds i Regeringskansliet.

För att skydda den personliga integriteten bör Säkerhetspolisens direktåtkomst vara så begränsad som möjligt. *Säkerhetspolisen* anser att myndigheten behöver ha direktåtkomst till såväl passregistret som passstillståndsregistret. Passstillståndsregistret innehåller dock särskilt integritetskänsliga uppgifter och det är svårt att se vilket konkret behov Säkerhetspolisen har av uppgifterna i det registret. Direktåtkomst bör därför kunna medges endast till personuppgifter i passregistret. Det bör vidare uttryckligen anges att eventuell direktåtkomst ska vara begränsad till de uppgifter i passregistret som Säkerhetspolisen behöver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Denna begränsning av åtkomsten kan regleras i passdataförordningen.

Genom direktåtkomsten får Säkerhetspolisen direkt tillgång till passregistret. De sökförbud som har föreslagits i avsnitt 6.11 bör därför gälla även för Säkerhetspolisen. Det blir därmed förbjudet för Säkerhetspolisen att utföra sökningar i passregistret i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning, dvs. personuppgifter som rör lagöverträdelse och straffprocessuella tvångsmedel. Det blir också förbjudet för Säkerhetspolisen att söka i passregistret med hjälp av bl.a. ansiktsbilder. Dessa begränsningar av myndighetens sökmöjligheter bör framgå direkt av lagen.

Någon annan direktåtkomst bör inte vara tillåten

Kustbevakningen, Tullverket och Migrationsverket kan på olika sätt medverka i den gränskontroll som Polismyndigheten har ansvar för (jfr 5 a § passlagen och 9 kap. 1 § utlänningslagen). För att kunna göra detta kan myndigheterna behöva ta del av personuppgifter från passverksamheten. Detta är till stor del möjligt enligt gällande rätt. Uppgifter som inte omfattas av sekretess ska på begäran i regel lämnas ut till myndigheterna och enligt 23 § passförordningen ska Polismyndigheten lämna ut fotografier av enskilda från passregistret till Kustbevakningen och Tullverket. Den personuppgiftsbehandling som krävs för utlämnande har i båda fallen stöd i den sekundära ändamålsbestämmelse som har föreslagits i avsnitt 6.6.5. I många fall kommer uppgifterna att kunna lämnas ut elektroniskt på annat sätt än genom direktåtkomst, enligt förslaget i början av detta avsnitt.

Det har inte kommit fram annat än att dessa bestämmelser är tillräckliga för att tillgodose Kustbevakningens, Tullverkets och Migrationsverkets behov av uppgifter från passverksamheten. Något förslag om direktåtkomst lämnas därför inte. Det har inte heller i övrigt kommit fram att någon aktör har ett sådant behov av uppgifter från passverksamheten att direktåtkomst bör kunna medges. Den föreslagna regleringen bör därför vara uttömmande.

6.13 Sekretessbrytande uppgiftsskyldighet

Förslag: En passmyndighet eller Regeringskansliet (Utrikesdepartementet) ska vid direktåtkomst ha rätt att ta del av personuppgifter som en annan passmyndighet eller Regeringskansliet (Utrikesdepartementet) behandlar. Säkerhetspolisen ska vid direktåtkomst ha rätt att ta del av personuppgifter i passregistret.

Liksom i dag ska Polismyndigheten på begäran lämna ut en bild från passregistret till vissa myndigheter. Bestämmelsen om detta ska föras över från passförordningen till passdatalagen.

Bedömning: Uppgifter om ett pass giltighet är offentliga. Det behövs därför inte någon sekretessbrytande bestämmelse för att uppgifterna ska kunna lämnas ut genom direktåtkomst.

Den tidigare promemorians förslag överensstämmer med förslaget här när det gäller Polismyndighetens skyldighet att lämna ut bilder. Promemorian innehåller däremot inget förslag om sekretessbrytande uppgiftsskyldighet i samband med direktåtkomst.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Ekobrottsmyndigheten* anser dock att Polismyndigheten på begäran ska vara skyldig att lämna ut även namnteckningar från passregistret. Namnteckningar används enligt myndigheten som jämförelsematerial i vissa brottsutredningar.

Skälen för förslaget och bedömningen

Sekretess för uppgifter i passverksamheten

Passverksamheten är sekretessreglerad. Bestämmelser om sekretess för uppgifter i passregistret finns i 22 kap. 1 § offentlighets- och sekretesslagen jämförd med 6 § offentlighets- och sekretessförordningen. Bestämmelser om sekretess för uppgifter i enskilda passärenden finns i 35 kap. 22 § offentlighets- och sekretesslagen.

Sekretessbestämmelserna har beskrivits i avsnitt 3.4.4. För en uppgift i passregistret om en enskilds personliga förhållanden gäller sekretess endast om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs. För en fotografisk bild i passregistret gäller däremot

sekretess om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

För uppgifter om en eskilds personliga förhållanden i ett ärende enligt passlagen gäller sekretess om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Denna sekretess gäller dock inte för uppgifter som finns i ett beslut.

Direktåtkomst kan kräva sekretessbrytande bestämmelser

Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar inte beslut om utlämnande i varje enskilt fall. Prövningen av om ett utlämnande är förenligt med offentlighets- och sekretesslagen måste därför ske redan när uppgifterna görs tillgängliga genom direktåtkomst, oavsett om någon mottagare tar del av dem vid den tidpunkten. En bestämmelse om direktåtkomst är inte i sig en sådan sekretessbrytande regel som avses i offentlighets- och sekretesslagen, eftersom bestämmelser om direktåtkomst bara tar sikte på formen för utlämnande. En förutsättning för att direktåtkomst ska kunna tillåtas är därför att åtkomsten bara avser offentliga uppgifter eller att den avser sådana sekretessbelagda uppgifter som enligt lag eller förordning får lämnas ut till den som har direktåtkomst.

Bestämmelser om direktåtkomst till sekretessbelagda uppgifter brukar mot denna bakgrund kompletteras med sekretessbrytande bestämmelser som är utformade som regler om uppgiftsskyldighet. Dessa regler formuleras ofta som en rätt för mottagaren att ta del av uppgifter. Utlämnande genom direktåtkomst kan i vissa fall i och för sig ske med stöd av den sekretessbrytande generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen. Där föreskrivs att uppgifter får lämnas ut till en annan myndighet, trots sekretess, om det vid en bedömning är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda. Det har dock ansetts olämpligt att ett omfattande utlämnande av sekretessbelagda uppgifter sker enbart med stöd av generalklausulen.

Uppgifter om passhandlingars giltighet bedöms vara offentliga

I avsnitt 6.12.2 har det föreslagits att uppgift om ett pass giltighet ska få lämnas ut genom direktåtkomst. Uppgiften, dvs. att ett pass

är giltigt eller inte, ska enligt förslaget få lämnas ut till alla kategorier av mottagare, både myndigheter och enskilda. Det är fråga om en uppgift som finns i passregistret. Uppgiften får anses avse en enskilds personliga förhållanden men är harmlös. Det kan inte i något fall av särskild anledning antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs. Uppgiften omfattas därmed inte av sekretess enligt 22 kap. 1 § offentlighets- och sekretesslagen jämförd med 6 § offentlighets- och sekretessförordningen. Eftersom uppgiften är offentlig behövs det inte någon sekretessbrytande bestämmelse för att möjliggöra direktåtkomsten. Det kan konstateras att inte heller bestämmelsen om direktåtkomst i 16 § lagen om identitetskort för folkbokförda i Sverige kompletteras av någon sekretessbrytande bestämmelse. Sekretesskyddet för uppgifter i databasen över identitetskort för folkbokförda i Sverige är enligt 6 § offentlighets- och sekretessförordningen detsamma som för uppgifter i passregistret.

Annan direktåtkomst förutsätter sekretessbrytande bestämmelser

I avsnitt 6.12.2 har det föreslagits att passmyndigheterna och Utrikesdepartementet ska kunna medge varandra direktåtkomst till personuppgifter i passverksamheten. Det har också föreslagits att Säkerhetspolisen ska få medges direktåtkomst till passregistret.

I passregistret och passverksamheten i övrigt behandlas uppgifter som i vissa fall omfattas av sekretess. Det handlar framför allt om de fotografier som finns i passregistret men även uppgifter om t.ex. psykiatrisk vård kan omfattas av sekretess (jfr avsnitt 3.4.4).

Det är inte lämpligt att de sekretessbelagda uppgifterna lämnas ut genom direktåtkomst endast med stöd av generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen. Särskilda sekretessbrytande bestämmelser bör i stället tas in i den nya lagen. Dessa bör utformas som en rätt för den mottagande myndigheten att ta del av uppgifter.

En sekretessbrytande bestämmelse som gäller i enskilda fall

De sekretessbrytande bestämmelserna ovan föreslås gälla i samband med direktåtkomst. Sekretessbelagda uppgifter bör dock i vissa fall kunna lämnas ut till andra myndigheter även när det inte är fråga om

direktåtkomst. En bestämmelse som möjliggör det finns i dag i 23 § andra stycket passförordningen. Polismyndigheten ska enligt den bestämmelsen på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen, Ekobrottsmyndigheten, svensk ambassad, svenskt lönat konsulat, Försvarsmakten, Kustbevakningen, Tullverket, Skatteverket och Kronofogdemyndigheten.

För att hålla samman regleringen i fråga om uppgiftsskyldighet bör bestämmelsen i 23 § andra stycket passförordningen föras över till passdatalagen. För att fotografier i passregistret ska kunna lämnas ut till Säkerhetspolisen även på annat sätt än via direktåtkomst bör myndigheten nämnas som mottagare även i fortsättningen.

Något skäl att utöka uppgiftsskyldigheten till att omfatta andra uppgifter än bilderna i passregistret har inte kommit fram. Efter en prövning i det enskilda fallet kan andra sekretessbelagda uppgifter i verksamheten lämnas ut med stöd av generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen. Den enskildes namnteckning, som *Ekobrottsmyndigheten* nämner, omfattas av sekretess bara om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs. Det innebär att namnteckningen i regel är offentlig och ska lämnas ut om en annan myndighet begär det (6 kap. 5 § offentlighets- och sekretesslagen).

6.14 Bevarande och gallring

Förslag: Uppgifter och handlingar i passregistret ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna gäller avslutades.

Regeringen eller den myndighet som regeringen bestämmer ska kunna meddela föreskrifter om att uppgifter och handlingar i passregistret får bevaras längre tid än tio år för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål. Om uppgifter och handlingar bevaras för sådana ändamål ska de avskiljas från den löpande passverksamheten. Åtkomsten till uppgifterna och handlingarna ska begränsas.

De fingeravtryck som tas i samband med en passansökan och de biometriska uppgifter som tas fram ur fingeravtrycken ska på samma sätt som i dag omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Bestämmelsen om detta ska dock föras över från passlagen till passdatalagen.

En chefsöverläkare ska underrätta Polismyndigheten i vissa fall när en person inte längre är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård, för att möjliggöra att uppgifter och handlingar i passstillståndsregistret kan gallras i rätt tid.

Bedömning: Några andra regler om gallring bör inte införas. Enligt dataskyddsförordningen får personuppgifter bevaras så länge det är nödvändigt med hänsyn till ändamålen med behandlingen. Om personuppgifterna behandlas enbart för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får de bevaras under längre tid.

Den tidigare promemorians förslag överensstämmer delvis med förslaget här. I promemorian föreslås en generell bestämmelse om att uppgifter ska gallras så snart de inte längre behövs för något av de ändamål som de behandlas för. Någon särskild bestämmelse om gallring av uppgifter i passregistret föreslås inte. Däremot föreslås en bestämmelse om gallring av uppgifter i passstillståndsregistret. Det föreslås också att Socialstyrelsen ska vara skyldig att underrätta Polismyndigheten i vissa fall när en person inte längre är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård, för att uppgifter och handlingar i passstillståndsregistret ska kunna gallras i rätt tid.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inga invändningar mot förslaget. *Datainspektionen* anser dock att en ändamålsanknuten gallringsbestämmelse riskerar att bli för vag och otillräcklig för att tillgodose integritetsskyddsintresset i passverksamheten. Inspektionen förordar bestämda tidsfrister för gallring av uppgifter. *Riksarkivet* anser att utgångspunkten vad gäller bevarande och gallring borde vara arkivlagstiftningen snarare än särskilda gallringsbestämmelser i disparata registerförfattningar. Riksarkivet anser att integritetskänsliga uppgifter bör skyddas med hjälp av sekretessbestämmelser snarare än med gallringsföreskrifter. *Socialstyrelsen* avstyrker förslaget att Socialstyrelsen ska underrätta Polismyndigheten i vissa fall när en person inte längre är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård. Socialstyrelsen anger att myndigheten saknar kännedom om utskrivningar och att underrättelseskyldigheten i stället bör ligga på chefsöverläkaren.

Skälen för förslaget och bedömningen

Olika perspektiv på hur länge information ska bevaras

Frågan om hur länge personuppgifter får behandlas är viktig och samtidigt komplex. Från verksamhetssynpunkt finns det inte sällan fördelar med att kunna bevara personuppgifter under förhållandevis lång tid. Från integritetsperspektiv kan detta medföra risker. I den mån personuppgifterna finns i allmänna handlingar, vilket är vanligt i myndigheternas verksamhet, gör sig ytterligare intressen gällande. Offentlighetsprincipen bygger till stor del på att myndigheterna bevarar allmänna handlingar, så att allmänheten kan ta del av dem även när de har förlorat sin omedelbara nytta i verksamheten.

Dessa delvis motstående intressen kommer till uttryck även i lagstiftningen. Dataskyddsförordningen har som utgångspunkt att personuppgifter inte ska behandlas under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, i vart fall inte i en form som möjliggör identifiering av den registrerade. Den svenska arkivlagstiftningen har som utgångspunkt att allmänna handlingar ska bevaras, även om de innehåller personuppgifter.

Dataskyddsförordningen ställer krav på lagringsminimering

Lagring av personuppgifter, genom arkivering eller på något annat sätt, är en behandling som omfattas av dataskyddsförordningen. Detta gäller under förutsättning att lagringen är helt eller delvis automatiserad eller att personuppgifterna ingår i eller kommer att ingå i ett register. Behandling för arkivändamål av allmänt intresse är generellt sett laglig, eftersom behandlingen anses vara förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Detta framgår av artikel 5.1 b i förordningen (se vidare avsnitt 6.6.6).

Av artikel 5.1 e i förordningen framgår dock att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Denna grundsats kallas för principen om lagringsminimering. För passverksamhetens del innebär principen att personuppgifter som utgångspunkt inte får bevaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för handläggning av passärenden eller något sekundärt ändamål. När personuppgifterna inte längre behövs för dessa ändamål ska de raderas eller överföras till en form som inte möjliggör identifiering av den registrerade.

Undantag vid behandling som följer av arkivlagstiftningen

Principen om lagringsminimering gäller inte utan undantag. Av artikel 5.1 e i dataskyddsförordningen framgår att personuppgifter får lagras under längre perioder än vad som är nödvändigt med hänsyn till ändamålet i den mån uppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. En förutsättning för detta är att lämpliga tekniska och organisatoriska åtgärder genomförs för att säkerställa den registrerades rättigheter och friheter.

Bestämmelser om bevarande av uppgifter genom arkivering av allmänna handlingar finns för svensk del i arkivlagen (1990:782), arkivförordningen (1991:446) och Riksarkivets föreskrifter (RA-FS och RA-MS). I propositionen Ny dataskyddslag (prop. 2017/18:105 s. 110) har regeringen uttalat att den behandling av personuppgifter som myndigheterna utför för att arkivera allmänna handlingar enligt arkivlagstiftningen måste anses ske för arkivändamål av allmänt

intresse i den mening som begreppet har i dataskyddsförordningen. Regeringen har i samma proposition (s. 116) uttalat att det skydd som enligt svensk rätt gäller för myndigheters arkiv, i synnerhet de sekretessbestämmelser som finns i offentlighets- och sekretesslagen, uppfyller dataskyddsförordningens krav på skyddsåtgärder.

Detta innebär att personuppgifter får bevaras under en längre tid än vad som framgår av principen om lagringsminimering, om den svenska arkivlagstiftningen kräver att uppgifterna ska bevaras.

Arkivlagstiftningen har som utgångspunkt att handlingar ska bevaras

Allmänna handlingar ska som huvudregel bevaras. Detta gäller oavsett om handlingarna innehåller personuppgifter eller inte. I vissa fall får allmänna handlingar ändå gallras. Med gallring menas att en handling på ett eller annat sätt förstörs. Vanliga pappershandlingar förstörs fysiskt. När det gäller elektroniska handlingar innebär gallring vanligtvis att information raderas från en databärare.

För statliga myndigheter gäller att allmänna handlingar får gallras i två fall. För det första får handlingar gallras om detta föreskrivs i en registerförfattning eller en annan lag eller förordning. Enligt 10 § tredje stycket arkivlagen har avvikande föreskrifter om gallring nämligen företrädde framför arkivlagen. För det andra får allmänna handlingar gallras om Riksarkivet har meddelat föreskrifter eller beslut om gallring. Saknas det stöd för gallring ska allmänna handlingar bevaras. Detta framgår av 14 § arkivförordningen.

Lagringsminimering och arkivering i passverksamheten

Utgångspunkten är att principen om lagringsminimering gäller i passverksamheten, enligt artikel 5.1 e i dataskyddsförordningen. Personuppgifter får alltså inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt med hänsyn till de ändamål för vilka personuppgifterna behandlas. Vad detta innebär, dvs. hur lång tid personuppgifter i praktiken får behandlas, är upp till den personuppgiftsansvarige att bedöma. Enligt uppgift från Polismyndigheten visar passregistret varje registrerads innehav av pass under de senaste ca tjugo åren.

När det gäller personuppgifter som ingår i allmänna handlingar är utgångspunkten som framgått att dessa ska bevaras, trots principen om lagringsminimering. Uppgifterna får gallras bara med stöd av lag eller förordning eller i enlighet med föreskrifter eller beslut som Riksarkivet har meddelat. Bestämmelser om gallring av handlingar i Polismyndighetens passärenden finns i Riksarkivets föreskrifter (RA-MS 2017:45) om bevarande och gallring hos Polismyndigheten. Av bilaga 1 till föreskrifterna framgår bl.a. att uppgifter i RES om indragning, återkallelse och förlustanmälan, samt elektroniska bilagor till en passansökan skapade genom skanning, får gallras ett år efter det att passets giltighetstid har gått ut. Uppgifter som utgör underlag för ett avslagsbeslut och makulerad ansökan får gallras fem år efter makuleringsdatum. Pappershandlingar som har skannats in i RES får gallras efter skanning. Enligt föreskrifterna får även vissa andra uppgifter gallras, bl.a. uppgifter om betalning av ansökningsavgift. Uppgifter som inte nämns i föreskrifterna ska bevaras.

Övriga passmyndigheter och Utrikesdepartementet använder RES-UM vid handläggningen av passärenden (jfr avsnitt 3.3.4). De personuppgifter som sparas i RES-UM förs till stor del över till Polismyndigheten och sparas i RES. Gallring sker därefter enligt de föreskrifter som har nämnts ovan. För ambassader och konsulat gäller även Regeringskansliets föreskrifter (RKF 2009:14, omtryck RKF 2015:5) om gallring av allmänna handlingar hos myndigheter inom utrikesrepresentationen. Där anges bl.a. att handlingar i allmänna passärenden får gallras efter tio år. Gallringen förutsätter ett medgivande av Regeringskansliets förvaltningsavdelning.

Det bör slutligen nämnas att de fingeravtryck som tas i samband med en passansökan ska förstöras omedelbart när passet har lämnats ut eller passansökan har återkallats eller avslagits (6 a § passlagen). Samma sak gäller de biometriska data som tas fram ur fingeravtryck och ansiktsbild under handläggningen. Även detta kan uppfattas som en gallringsbestämmelse. I avsnitt 6.10.4 har det föreslagits att bestämmelsen ska ändras så att de biometriska uppgifter som har tagits fram ur ansiktsbilden ska kunna sparas i passregistret. Syftet är att ansiktsbilder ska kunna jämföras biometriskt i samband med passansökningar. När det handlar om fingeravtrycken föreslås inga förändringar. De ska även i fortsättningen förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.

Flera alternativ är tänkbara om en passdatalag införs

När en passdatalag nu föreslås kan frågan om bevarande och gallring hanteras på olika sätt. Det finns åtminstone tre olika alternativ.

Det första alternativet är att låta allmänna principer gälla och inte införa några särskilda bestämmelser om gallring. Passmyndigheterna och Utrikesdepartementet får då som utgångspunkt själva bedöma hur länge personuppgifter får behandlas i en form som möjliggör identifiering, utifrån principen om lagringsminimering. I den mån uppgifterna ingår i allmänna handlingar gäller arkivlagstiftningen, vilket innebär att uppgifterna ska bevaras om de inte får gallras.

Det andra alternativet är att så långt som möjligt införa särskilda bestämmelser om hur länge personuppgifter får behandlas. Enligt artikel 6.2 och 6.3 i dataskyddsförordningen får medlemsstaterna införa bestämmelser om lagringstider, när behandlingen grundar sig på artikel 6.1 c eller 6.1 e. Behandlingen av personuppgifter i passverksamheten grundar sig på dessa artiklar (jfr avsnitt 5.4). I registerförfattningar på dataskyddsförordningens område utformas bestämmelser om lagringstider i regel som gallringsbestämmelser. Passdatalagen skulle kunna förses med sådana bestämmelser.

Det tredje alternativet är att som utgångspunkt låta de allmänna principerna gälla men att införa vissa bestämmelser om gallring, t.ex. när det handlar om uppgifter och handlingar i passregistret. En sådan lösning innebär att passmyndigheterna och Utrikesdepartementet som utgångspunkt tillämpar principen om lagringsminimering och, när det gäller personuppgifter som finns i allmänna handlingar, arkivlagstiftningen. På vissa områden, t.ex. i fråga om passregistret, skulle passdatalagen däremot innehålla särskilda bestämmelser om gallring av det slag som har företrädare framför arkivlagstiftningen.

Det finns fördelar och nackdelar med alla alternativ. Från ett integritetsperspektiv kan lagstadgade gallringsfrister framstå som önskvärda. Tydliga gallringsbestämmelser gör det lätt för såväl den registrerade som för de berörda myndigheterna att överblicka hur länge personuppgifter får behandlas. Sannolikt underlättas också tillsynen. *Datainspektionen* förespråkar bestämda gallringsfrister. Det finns samtidigt fördelar med att låta den allmänna principen om lagringsminimering gälla, tillsammans med arkivlagstiftningen. Det medför sannolikt att fler handlingar och uppgifter kan bevaras, med stöd av arkivlagstiftningens huvudregel, vilket ökar allmänhetens

möjligheter till insyn i verksamheten. Som *Riksarkivet* påpekar är det inte heller givet att gallring alltid är till fördel för den enskilde. Att uppgifter bevaras kan vara en förutsättning för att den enskilde ska kunna få insyn i ett ärende och kunna bevaka sina intressen.

Ingen generell gallringsbestämmelse i passdatalagen

Det lämpligaste för passverksamhetens del är rimligen att även i fortsättningen låta den allmänna principen om lagringsminimering vara utgångspunkten för hur länge personuppgifter får behandlas. Detta är vad som föreslås i den tidigare promemorian och de flesta remissinstanser tillstyrker eller har inga invändningar mot förslaget. Principen innebär som redan framgått att passmyndigheterna och Utrikesdepartementet inte får förvara personuppgifter i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för handläggning av passärenden eller för något sekundärt ändamål. Någon särskild lagbestämmelse behövs inte eftersom principen framgår direkt av dataskyddsförordningen.

Även när det handlar om personuppgifter som ingår i allmänna handlingar bör utgångspunkten vara den som följer av gällande rätt, dvs. att arkivlagstiftningen styr om uppgifterna ska bevaras eller gallras. Av artikel 5.1 e i dataskyddsförordningen följer som framgått att personuppgifter får lagras under längre perioder i den mån uppgifterna enbart behandlas för arkivändamål av allmänt intresse. Som regeringen påpekat i propositionen *Ny dataskyddslag* (prop. 2017/18:105 s. 116) finns det också lämpliga skyddsåtgärder.

Någon generell bestämmelse om gallring bör alltså inte införas i passdatalagen. Med hänsyn till framför allt integritetsintresset finns det emellertid skäl att överväga särskilda gallringsbestämmelser i fråga om passregistret, passtillståndsregistret och fingeravtryck.

Uppgifter i passregistret bör normalt gallras efter tio år

Passregistret innehåller uppgifter om ett stort antal människor. En stor del av den svenska befolkningen är registrerad. Många av de uppgifter som behandlas framstår visserligen som harmlösa men även uppgifter av mer integritetskänsligt slag, som ansiktsbilder, behandlas. I denna promemoria föreslås att även sådana biometriska

uppgifter som har tagits fram ur ansiktsbilder ska få sparas i registret. Det föreslås vidare att uppgifter i passregistret ska få användas för sekundära ändamål som gränskontroll och brottsbekämpning och att Säkerhetspolisen ska kunna medges direktåtkomst till registret.

För att skydda den registrerades personliga integritet, underlätta de personuppgiftsansvarigas arbete och skapa goda förutsättningar för tillsyn bör en särskild gallringsfrist införas för handlingar och uppgifter i passregistret. En sådan frist får som framgått införas i nationell rätt enligt artikel 6.2 och 6.3 i dataskyddsförordningen.

Frågan är då vilken gallringsfrist som bör gälla. Det kan noteras att förhållandevis korta frister gäller på vissa närliggande områden. Enligt 17 § förordningen om nationellt identitetskort ska en uppgift i registret över nationella identitetskort gallras senast sex månader efter det att giltighetstiden för ett identitetskort har gått ut. Enligt 13 § förordningen (2015:904) om identitetskort för folkbokförda i Sverige ska uppgifter och handlingar i regel gallras senast ett år efter det att giltighetstiden för ett identitetskort har gått ut.

En gallringsfrist på sex månader eller ett år det att giltighetstiden för ett pass har gått ut framstår emellertid som alltför snäv för att passregistret ska kunna fylla sin funktion. För att registret ska kunna användas på ett ändamålsenligt sätt när passärenden handläggs bör gallringsfristen vara något längre. I Regeringskansliets föreskrifter om gallring av allmänna handlingar hos myndigheter inom utrikesrepresentationen anges att handlingar i passärenden får gallras efter tio år. Tio år är också den tid som uppgifter i Migrationsverkets register över fingeravtryck och fotografier som längst får bevaras. Detta framgår av 3 § utlänningsdataförordningen (2016:30).

En tioårig frist skulle för passregistrets del innebära att registret kan visa handlingar och uppgifter från de två senaste passärendena, förutsatt att passinnehavaren ansöker om nytt pass i anslutning till att det gamla löper ut. Den ansiktsbild av sökanden som tas vid en passansökan kommer, i enlighet med förslaget i avsnitt 6.10.4, att kunna jämföras med andra ansiktsbilder som har tagits under de senaste tio åren. Något tungt vägande skäl för att bevara handlingar eller uppgifter i passregistret längre tid än så har inte kommit fram.

Frågan är då från vilken tidpunkt fristen bör räknas. Passregistret bör, enligt förslaget i avsnitt 6.9.2, få innehålla uppgifter om både personer som har beviljats pass och personer som har varit parter i passärenden utan att få pass. Det går därför inte att knyta fristen till

utfärdandet av ett pass eller till passets giltighetstid. Det bör i stället införas en bestämmelse som anger att uppgifter och handlingar i passregistret ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades. Uppgifter och handlingar får därmed sparas under tio år räknat från utgången av det år då ett pass utfärdades, en passansökan avslogs eller återkallades eller ärendet avslutades på annat sätt.

Det kan finnas goda skäl för att vissa handlingar eller uppgifter i passregistret ska kunna bevaras under en längre tid än tio år, för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål. En absolut gallringsfrist som inte ger utrymme för detta framstår som olämplig. Regeringen eller den myndighet som regeringen bestämmer bör därför kunna meddela föreskrifter om att uppgifter och handlingar i passregistret får bevaras under en längre tid än tio år, om det sker för de angivna ändamålen. Det är samtidigt viktigt att gallringsfristen får det genomslag som är avsett. Det bör därför införas en bestämmelse som anger att uppgifter och handlingar som bevaras under en längre tid än tio år för exempelvis arkivändamål ska avskiljas från den löpande passverksamheten. Åtkomsten till uppgifter och handlingar som avskiljs bör dessutom begränsas till särskilt angivna tjänstemän. Dessa bestämmelser om avskiljande och åtkomst kan tas in i passdataförordningen.

Uppgifter i passtillståndsregistret kommer att gallras löpande

Vid sidan av passregistret föreslås att Polismyndigheten liksom i dag ska föra ett register över omständigheter som avses i 20 § 1 och 3 passlagen (jfr avsnitt 6.9). De omständigheter som avses där är att passtillstånd krävs för den som är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård, för att chefsöverläkaren har anmält att pass inte får utfärdas utan ett sådant tillstånd eller att ett tidigare pass efter intagningen har återkallats på ett visst sätt. Det föreslås att registret i fortsättningen ska kallas för passtillståndsregistret.

Den reglering som föreslås innebär att registret kan komma att innehålla känsliga personuppgifter. Det talar för att uppgifterna inte ska bevaras under en längre tid än vad som är absolut nödvändigt. Någon särskild gallringsbestämmelse behövs dock inte för att detta ska gälla. Enligt förslaget ska passtillståndregistret bara få innehålla

de uppgifter som är nödvändiga för att det ska kunna avgöras om passstillstånd krävs för en person enligt 20 § 1 eller 3 passlagen. När en person inte längre är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård krävs inte längre passstillstånd. Passstillstånd krävs inte heller om chefsöverläkaren återkallar sin anmälan. Det följer då av principen om lagringsminimering att personuppgifterna i registret ska raderas eller överföras till en form som inte möjliggör identifiering. Uppgifterna i registret ska således gallras löpande, så snart det visar sig att passstillstånd inte längre krävs för en person.

För att uppgifterna i registret ska kunna gallras i rätt tid krävs det att Polismyndigheten får information om att en viss person inte längre är intagen för psykiatrisk tvångsvård eller rättspsykiatrisk vård. För att säkerställa att Polismyndigheten får denna information bör det införas vissa bestämmelser om underrättelseskyldighet i passförordningen. I den tidigare promemorian föreslogs det att denna underrättelseskyldighet skulle ligga på Socialstyrelsen. Som *Socialstyrelsen* påpekar är det dock i första hand chefsöverläkaren som känner till att en viss patient har skrivits ut. Skyldigheten att underrätta Polismyndigheten bör alltså ligga på chefsöverläkaren.

Fingeravtryck bör liksom i dag gallras när ärendet har avslutats

De fingeravtryck som tas vid en passansökan, och de biometriska uppgifter som tas fram ur dessa, ska enligt 6 a § passlagen omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Fingeravtrycken får alltså inte sparas någon annanstans än i passet. I förarbetena till bestämmelsen angavs att det därmed inte finns någon möjlighet att bygga upp ett separat fingeravtrycksregister med hjälp av de fingeravtryck som lämnas vid passansökningar (prop. 2008/09:132 s. 16). Någon ändring i detta avseende föreslås inte i denna promemoria. Bestämmelsen om att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa ska förstöras när ärendet har avslutats bör dock föras över från passlagen till passdatalagen, så att reglerna om bevarande och gallring finns samlade. Kravet på att fingeravtrycken och de biometriska uppgifterna ska förstöras bör även i fortsättningen vara absolut. Det bör alltså inte kunna meddelas några föreskrifter om att uppgifterna får bevaras för exempelvis arkivändamål av allmänt intresse.

6.15 Tillsyn, överklagande och skadestånd

Bedömning: Lagen behöver inte innehålla några bestämmelser om tillsyn, överklagande av beslut eller skadestånd.

Den tidigare promemorians bedömning överensstämmer med bedömningen här, förutom att det föreslås en bestämmelse om att personuppgiftslagens regler om skadestånd ska gälla.

Remissinstanserna tillstyrker eller har inga invändningar mot bedömningen och förslaget.

Skälen för bedömningen: Dataskyddsförordningen innehåller bestämmelser om oberoende tillsynsmyndigheter (kapitel VI) samt rättsmedel, ansvar och sanktioner (kapitel VIII). Dataskyddslagen innehåller kompletterande bestämmelser om tillsynsmyndighetens handläggning och beslut (6 kap.) samt skadestånd och överklagande (7 kap.). Vissa ytterligare föreskrifter finns i förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning.

Regelverket innebär att Datainspektionen är tillsynsmyndighet enligt dataskyddsförordningen och dataskyddslagen. Det behövs inga bestämmelser i passdatalagen för att tillsynen ska omfatta den behandling av personuppgifter som utförs i passverksamheten.

Enligt artikel 83 i dataskyddsförordningen ska sanktionsavgifter kunna tas ut vid vissa överträdelser av förordningen. Enligt artikel 83.7 är det upp till varje medlemsstat att avgöra om även offentliga myndigheter ska kunna påföras sanktionsavgifter. Av 6 kap. 2 § dataskyddslagen framgår att sanktionsavgifter i Sverige kan tas ut även av myndigheter. Det finns inte skäl att göra undantag från den ordningen vid personuppgiftsbehandling enligt passdatalagen.

Beslut som en personuppgiftsansvarig myndighet meddelar med anledning av att en registrerad utövar sina rättigheter enligt dataskyddsförordningen får enligt 7 kap. 2 § dataskyddslagen överklagas till allmän förvaltningsdomstol. Detta gäller beslut enligt artiklarna 12.5 och 15–21 i dataskyddsförordningen. Andra beslut som en personuppgiftsansvarig myndighet fattar enligt dataskyddsförordningen får enligt 7 kap. 5 § dataskyddslagen inte överklagas. De bestämmelser som föreslås i denna promemoria medför inte att det kommer att fattas några andra beslut som bör kunna överklagas än de som anges i dataskyddslagen. Den nya lagen behöver därför inte innehålla några bestämmelser om överklagande av beslut.

Enligt artikel 82.1 i dataskyddsförordningen ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. En kompletterande bestämmelse finns i 7 kap. 1 § dataskyddslagen. Där anges att rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet enligt artikel 82 i dataskyddsförordningen gäller vid överträdelser av bestämmelser i dataskyddslagen och andra föreskrifter som kompletterar dataskyddsförordningen. Passdatalagen föreslås innehålla sådana föreskrifter som kompletterar dataskyddsförordningen. Rätten till skadestånd enligt artikel 82 i förordningen kommer därför att gälla vid överträdelser av lagen eller föreskrifter som har meddelats i anslutning till lagen. Mot den bakgrunden behövs det inga bestämmelser om skadestånd i lagen.

7 Sekretess för biometriska uppgifter

Förslag: Sekretess ska gälla för biometriska uppgifter i passregistret som har tagits fram ur en fotografisk bild av en enskild, om det inte står klart att uppgifterna kan röjas utan att den enskilde eller någon närstående till denne lider men.

Den tidigare promemorian innehåller inget förslag i frågan.

Remissinstanserna yttrar sig inte i frågan.

Skälen för förslaget: Vilken sekretess som gäller för uppgifter i passverksamheten har beskrivits i avsnitt 3.4.4. För fotografierna i passregistret gäller en presumtion för sekretess. De får lämnas ut bara om det står klart att de kan röjas utan att den enskilde eller någon närstående till denne lider men. För andra uppgifter i passregistret och i passärenden råder en presumtion för offentlighet. Någon särskild bestämmelse om biometriska uppgifter finns inte.

De biometriska uppgifter som tas fram ur fingeravtryck och ansiktsbilder förstörs enligt dagens regelverk när passet har lämnats ut eller passansökan har återkallats eller avslagits (6 a § andra stycket passlagen). Denna ordning har analyserats från sekretessynpunkt tidigare (prop. 2004/05:119 s. 43–46). De biometriska uppgifter som tas fram innan passet utfärdas anses utgöra en mellanprodukt till det färdiga passet. Sådana handlingar blir inte allmänna om de inte expedieras eller tas om hand för arkivering (2 kap. 12 § andra stycket tryckfrihetsförordningen). Eftersom de biometriska uppgifterna varken expedieras eller arkiveras blir frågan om sekretess inte aktuell.

När det gäller fingeravtrycken och de biometriska uppgifter som tas fram ur dessa föreslås inga ändringar i denna promemoria. Dessa uppgifter ska även i fortsättningen förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Uppgifterna blir

därför, i enlighet med den tidigare analysen, inte att betrakta som allmänna handlingar och frågan om sekretess blir inte aktuell.

När det gäller ansiktsbilderna och de biometriska uppgifter som tas fram ur dessa är läget annorlunda. I avsnitt 6.9.2 och 6.10.4 föreslås att både ansiktsbilderna och de biometriska uppgifter som har tagits fram ur dessa ska kunna sparas i passregistret. När de biometriska uppgifterna sparas i passregistret måste det antas att de blir allmänna handlingar. Det är fråga om upptagningar som förvaras hos Polismyndigheten. Upptagningarna kan i och för sig inte anses vara inkomna till myndigheten i tryckfrihetsförordningens mening, eftersom det är myndigheten själv som har tagit fram de biometriska uppgifterna (prop. 2004/05:119 s. 45). I och med lagringen i registret får de däremot anses ha upprättats enligt 2 kap. 10 § andra stycket 1 tryckfrihetsförordningen. Där anges att diaries, journaler samt sådana register eller andra förteckningar som förs fortlöpande anses ha upprättats när de har färdigställts för anteckning eller införing. Information som förs in i en sådan förteckning blir omedelbart en allmän handling, oavsett om det är fråga om en mellanprodukt eller inte (se rättsfallet HFD 2013 ref. 33). Om passregistret inte skulle betraktas som en sådan förteckning som förs fortlöpande får de biometriska uppgifterna ändå anses ha tagits om hand för arkivering genom lagringen i passregistret. De är då att betrakta som allmänna handlingar enligt 2 kap. 12 § andra stycket tryckfrihetsförordningen.

Utgångspunkten måste alltså vara att de biometriska uppgifter som har tagits fram ur ansiktsbilderna och som sparas i passregistret blir allmänna handlingar. Uppgifterna är integritetskänsliga och bör omfattas av en presumtion för sekretess på samma sätt som fotografierna i registret. Frågan är om nya sekretessbestämmelser krävs för att de biometriska uppgifterna ska få ett sådant skydd.

Det skulle kunna argumenteras för att den sekretess som gäller för fotografierna i passregistret, enligt 22 kap. 1 § offentlighets- och sekretesslagen och 6 § offentlighets- och sekretessförordningen, omfattar även de biometriska uppgifter som har tagits fram ur fotografierna. Detta är dock inte givet. De bestämmelser som föreslås innebär att de biometriska uppgifterna kan sparas antingen som en del av fotografierna eller självständigt. För att det inte ska råda något tvivel om att presumtionen för sekretess gäller, oavsett hur uppgifterna sparas rent tekniskt, bör bestämmelserna i 22 kap. 1 § offentlighets- och sekretesslagen och 6 § offentlighets- och

sekretessförordningen ändras. Av bestämmelserna bör framgå att sekretess gäller både för fotografiska bilder av enskilda i passregistret och för biometriska uppgifter som har tagits fram ur sådana bilder, om det inte står klart att uppgifterna kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

Bestämmelserna i 22 kap. 1 § offentlighets- och sekretesslagen och 6 § offentlighets- och sekretessförordningen gäller inte bara för uppgifter i passregistret. De gäller också för bl.a. folkbokföringen, Transportstyrelsens vägtrafikregister och vissa andra register. I den mån biometriska uppgifter tas fram ur fotografier av enskilda i dessa register kommer även de uppgifterna att omfattas av sekretess till följd av den ändring som nu föreslås. Detta framstår som rimligt. De biometriska uppgifter som tas fram ur ett fotografi torde även i dessa sammanhang vara lika skyddsvärda som själva fotografiet.

8 Ikraftträdande- och övergångsbestämmelser

Förslag: Författningsförslagen ska träda i kraft den 1 juli 2020.

Bedömning: Det behövs inte några övergångsbestämmelser.

Den tidigare promemorians förslag och bedömning överensstämmer delvis med förslaget och bedömningen här. I promemorian föreslås, förutom en annan dag för ikraftträdande, att bestämmelsen om gallring av uppgifter som inte längre behövs inte ska behöva börja tillämpas förrän ett år efter ikraftträdandet.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget och bedömningen.

Skälen för förslaget och bedömningen: Det är angeläget att personuppgiftsbehandlingen i passverksamheten regleras närmare utan större tidsutdräkt. Författningsförslagen bör därför träda i kraft så snart som möjligt. Med hänsyn till den tid som kan antas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling framstår det som att den 1 juli 2020 är den tidigaste tidpunkt då författningsförslagen kan träda i kraft.

I den tidigare promemorian föreslås en bestämmelse om att uppgifter ska gallras så snart de inte längre behövs för något av de ändamål som de behandlas för (jfr avsnitt 6.14). Bestämmelsen kommer enligt promemorian att förutsätta ett visst utrednings- och systemutvecklingsarbete hos framför allt Polismyndigheten. För att medge tid för sådant arbete föreslås det att bestämmelsen inte ska behöva börja tillämpas förrän ett år efter ikraftträdandet.

De bestämmelser om gallring som föreslås i denna promemoria har en annan utformning och innebörd än i den äldre promemorian. Det föreslås att uppgifter och handlingar i passregistret ska gallras senast efter tio år och att principen om lagringsminimering ska gälla

i verksamheten i övrigt (avsnitt 6.14). En bortre tidsgräns för hur länge uppgifter i passregistret får behandlas underlättar sannolikt när myndigheterna ska anpassa sina verksamheter till den nya lagen. Det medför att behovet av förberedelse tid minskar. Den princip som föreslås gälla i övrigt, principen om lagringsminimering, är inte ny. Kravet på att personuppgifter ska gallras eller överföras till en form som inte möjliggör identifiering av den registrerade gällde enligt personuppgiftslagen och gäller nu enligt dataskyddsförordningen. De föreslagna bestämmelserna om bevarande och gallring bör mot denna bakgrund kunna träda i kraft och börja tillämpas vid samma tidpunkt som övriga bestämmelser i lagen, dvs. den 1 juli 2020.

Frågan är då om det behövs särskilda övergångsbestämmelser till den nya lagen. I det sammanhanget bör det nämnas att passdatalagen inte ersätter någon annan särskild registerförfattning. Behandlingen av personuppgifter i passverksamheten reglerades före den 25 maj 2018 av de allmänna bestämmelserna i personuppgiftslagen. Sedan dess omfattas behandlingen i stället av dataskyddsförordningen.

För överklagande av beslut som en passmyndighet eller t.ex. Datainspektionen kan ha meddelat med stöd av personuppgiftslagen gäller fortfarande personuppgiftslagen. Detta framgår av punkt 6 i övergångsbestämmelserna till dataskyddslagen och behöver inte regleras i någon särskild övergångsbestämmelse till passdatalagen.

Något behov av övergångsbestämmelser finns inte heller i övrigt.

9 Konsekvenser av förslagen

Bedömning: Förslagen innebär en förstärkning av skyddet för den enskildes personliga integritet. De bidrar samtidigt till att motverka brottslighet. I ett inledande skede kan förslagen ge upphov till vissa kostnader för framför allt Polismyndigheten. Dessa kostnader ryms dock inom befintliga anslag. I övrigt har förslagen inga sådana konsekvenser som bör redovisas särskilt.

Den tidigare promemorians bedömning överensstämmer i allt väsentligt med bedömningen här. Konsekvenserna i fråga om bl.a. brottslighet redovisas dock inte särskilt i promemorian.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har inga invändningar mot bedömningen. *Sveriges advokatsamfund* anser emellertid, som framgått av tidigare kapitel, att vissa av förslagen kan medföra negativa konsekvenser för den personliga integriteten.

Skälen för bedömningen

Vad innebär förslagen och vem berörs av dem?

Den behandling av personuppgifter som sker i passverksamheten omfattas i dag inte av någon särskild registerförfattning. Passlagen och passförordningen innehåller ett fåtal bestämmelser som kan anses röra behandling av personuppgifter. I övrigt gäller de allmänna bestämmelserna i dataskyddsförordningen och dataskyddslagen. Avsaknaden av en specifik författningsreglering har kritiserats. Kritiken har framför allt handlat om att passregistret, som omfattar en stor del av den svenska befolkningen, är bristfälligt reglerat.

I denna promemoria föreslås en sådan författningsreglering som har efterfrågats, i form av en passdatalag med tillhörande förordning. När det gäller passregistret föreslås bestämmelser som klargör bl.a.

vilka personer som får registreras, vilka uppgifter som får registreras, vilka sökningar som är förbjudna och när uppgifter och handlingar ska gallras. Därutöver föreslås ett antal bestämmelser som ska gälla vid all behandling av personuppgifter i passverksamheten. Av dessa framgår bl.a. för vilka ändamål personuppgifter får behandlas, hur ansvaret för personuppgiftsbehandlingen är fördelat, när känsliga personuppgifter får behandlas och när personuppgifter får lämnas ut elektroniskt genom direktåtkomst eller på annat sätt. Det finns även förslag som gäller säkerhetsåtgärder till skydd för personuppgifter.

Förslagen har vissa konsekvenser både för enskilda och för det allmänna. När det gäller enskilda berörs i första hand alla som har eller ansöker om pass. Förslagen påverkar hur den information som samlas in om dessa personer får behandlas, exempelvis hur lång tid deras personuppgifter får bevaras. I viss mån kan även företag eller privatpersoner som vill ta del av uppgifter inom passverksamheten påverkas, t.ex. genom förslagen om elektroniskt utlämnande.

För det allmänna får förslagen konsekvenser framför allt för de myndigheter som ska tillämpa den nya författningsregleringen. Det handlar om Polismyndigheten, vissa ambassader och konsulat samt Utrikesdepartementet. Säkerhetspolisen påverkas av förslagen om direktåtkomst. Även andra myndigheter, som Datainspektionen, kan i viss mån beröras av den nya författningsregleringen.

Förslagen leder till ett starkare integritetsskydd

De grundläggande bestämmelserna om skydd för fysiska personer vid behandling av personuppgifter finns i dataskyddsförordningen. Passdatalagen föreslås innehålla bestämmelser som kompletterar dataskyddsförordningen, främst i form av olika preciseringar. Man kan säga att förslagen förtydligar hur dataskyddsförordningen ska tillämpas när personuppgifter behandlas inom passverksamheten.

Redan dessa preciseringar och förtydliganden innebär en viss förstärkning av skyddet för den enskildes personliga integritet. För både den enskilde och de berörda myndigheterna blir det tydligare vilka personuppgifter som får behandlas, vem som är ansvarig för behandlingen, hur länge personuppgifter får bevaras osv. För den enskilde blir det därigenom lättare att ta till vara de rättigheter som

regelverket ger. En särskild författningsreglering underlättar vidare vid tillsyn och annan granskning av personuppgiftsbehandlingen.

I flera avseenden föreslås ett starkare integritetsskydd än vad dataskyddsförordningen kräver. Det gäller bl.a. förslagen om när känsliga personuppgifter får behandlas (avsnitt 6.10.3), vilka sökningar som är förbjudna (avsnitt 6.11) och när personuppgifter får lämnas ut elektroniskt (avsnitt 6.12). En inskränkning av den registrerades rättigheter enligt förordningen föreslås bara när det gäller rätten att göra invändningar mot tillåten behandling (avsnitt 6.7). Den inskränkningen är tillåten enligt dataskyddsförordningen.

Den samlade bedömningen är att förslagen innebär en tydlig förstärkning av skyddet för den enskildes personliga integritet.

Förslagen bidrar till att motverka brottslighet

I promemorian föreslås att personuppgifter som har samlats in för handläggning av passärenden ska få behandlas av Polismyndigheten om det är nödvändigt för att bekämpa brott (avsnitt 6.6.4). Det föreslås också att Säkerhetspolisen ska kunna medges direktåtkomst till passregistret för vissa ändamål (avsnitt 6.12.2). Förslagen, som bedöms vara förenliga med dataskyddsförordningen, säkerställer att personuppgifter i passverksamheten kan användas av de polisiära myndigheterna när det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Förslagen motverkar missbruk av identitetshandlingar genom att tillåta biometriska jämförelser av ansiktsbilder i anslutning till en passansökan (avsnitt 6.10.4). Det kan därmed upptäckas om någon försöker skaffa pass under en felaktig identitet. Att lämna oriktiga uppgifter vid en passansökan kan i sig vara brottsligt. Felaktigt utfärdade pass används dessutom vid bedrägerier och andra brott. Även förslaget att möjliggöra tekniska jämförelser av ansiktsbilder bidrar alltså till att motverka och bekämpa brottslighet.

De ekonomiska konsekvenserna av förslagen

Förslagen i promemorian bedöms inte påverka kostnaderna eller intäkterna för kommuner, företag eller andra enskilda. Förslaget om en utökad underrättelseskyldighet för chefsöverläkare (avsnitt 6.14)

innebär ett utökat åtagande för landstingen jämfört med i dag men bedöms inte påverka landstingens kostnader annat än marginellt.

När det gäller de statliga myndigheter som påverkas av förslagen görs följande bedömning. Den passdatalag som föreslås bygger på befintlig reglering i dataskyddsförordningen och passlagstiftningen. Till stor del handlar förslagen om att precisera och förtydliga sådant som på ett eller annat sätt redan gäller. Förslagen är teknikneutrala och kräver, såvitt kan bedömas, inte att vare sig Polismyndigheten eller någon annan myndighet investerar i nya datorsystem. Det får ändå antas att förslagen i ett inledande skede kommer att ge upphov till vissa kostnader för t.ex. utredning, utbildning och anpassningar av datorsystem. Det är framför allt Polismyndigheten som kommer att behöva utföra en del arbete av detta slag. I viss utsträckning kan även utlandsmyndigheterna och Utrikesdepartementet komma att beröras. Kostnaderna bedöms dock inte vara större än att de ryms inom varje myndighets befintliga anslag. Motsvarande bedömning har gjorts i den tidigare promemorian och ingen remissinstans har invänt. Förslagen ger inte upphov till några nya löpande kostnader för de myndigheter som i första hand ska tillämpa den nya lagen.

Tillsynsmyndigheten, Datainspektionen, har redan tillsyn över den behandling av personuppgifter som sker i passverksamheten. Tillsynen kommer snarast att underlättas av den nya regleringen och förslagen bedöms alltså inte medföra ökade kostnader för tillsyn.

De bestämmelser som föreslås medför inte att det kommer att fattas några andra beslut som kan överklagas än de som redan anges i dataskyddslagen. Förslagen bedöms därför inte leda till ökade kostnader för de allmänna förvaltningsdomstolarna.

Inga konsekvenser i övrigt

Förslaget om en utökad underrättelseskyldighet för chefsöverläkare innebär ett utökat åtagande för landstingen men bedöms påverka den kommunala självstyrelsen i ytterst liten utsträckning. Förslagen bedöms inte ha betydelse för sysselsättning och offentlig service i olika delar av landet. De bedöms inte heller ha betydelse för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags. Förslagen bedöms slutligen

inte ha betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

10 Författningskommentar

10.1 Förslaget till passdatalag

Syftet med lagen

1 § Syftet med denna lag är att personuppgifter ska kunna behandlas på ett ändamålsenligt sätt i passverksamheten, samtidigt som människor skyddas mot att deras personliga integritet kränks vid sådan behandling.

Paragrafen anger det övergripande syftet med lagen. Övervägandena finns i avsnitt 6.1.

Av paragrafen framgår att syftet med lagen är dubbelt. Dels ska personuppgifter kunna behandlas på ett ändamålsenligt sätt i passverksamheten, dels ska människor skyddas mot att deras personliga integritet kränks vid sådan behandling. Bestämmelsen anger utgångspunkterna för regleringen i lagen men har ingen självständig rättslig betydelse. Vad som avses med passverksamhet anges i 2 §.

Ord och uttryck i lagen

2 § Med passverksamhet avses i denna lag verksamhet enligt passlagen (1978:302). Övriga ord och uttryck som används i lagen har samma betydelse som i passlagen.

Paragrafen anger vad som avses med vissa ord och uttryck i lagen. Övervägandena finns i avsnitt 6.2.

Med passverksamhet avses enligt bestämmelsen sådan verksamhet som bedrivs enligt passlagen (1978:302). Passverksamhet omfattar alltså utfärdande av pass, återkallelse av pass och annan verksamhet som har sin grund i passlagen. Även verksamhet som följer av närmare bestämmelser i passförordningen (1979:664) eller

föreskrifter på myndighetsnivå är att betrakta som passverksamhet, eftersom även den verksamheten ytterst har sin grund i passlagen.

Övriga ord och uttryck som används i lagen har samma betydelse som i passlagen. Det gäller bl.a. ordet passmyndighet.

Lagens tillämpningsområde

3 § Denna lag gäller när passmyndigheterna och Regeringskansliet (Utrikesdepartementet) behandlar personuppgifter i passverksamheten.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Paragrafen anger lagens tillämpningsområde. Övervägandena finns i avsnitt 6.3.

Av första stycket framgår att lagen gäller vid viss behandling av personuppgifter. Med begreppet personuppgift avses detsamma som i dataskyddsförordningen, dvs. varje upplysning som avser en identifierad eller identifierbar fysisk person. Även med behandling avses detsamma som i dataskyddsförordningen, dvs. en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter. Som exempel kan nämnas insamling, registrering, lagring, läsning, användning och utlämning.

Lagen gäller när passmyndigheterna och Utrikesdepartementet, som är en del av Regeringskansliet, behandlar personuppgifter i sin passverksamhet. Vilka myndigheter som är passmyndigheter anges i passlagen (1978:302). Polismyndigheten är passmyndighet inom landet medan vissa beskickningar och konsulat fullgör uppgifter som passmyndigheter i utlandet. Vad som avses med passverksamhet framgår av 2 §. Begreppet omfattar all verksamhet som har sin grund i passlagen. Därmed omfattas all verksamhet som gäller pass för svenska medborgare. Även verksamhet som avser pass för utländska medborgare eller personer som har förlorat eller inte kan styrka sitt svenska medborgarskap omfattas, om verksamheten har sin grund i passlagen. Det innebär att lagen gäller exempelvis vid behandling av personuppgifter i ett ärende om provisorisk resehandling enligt förordningen (1997:698) om Europeiska unionens provisoriska resehandling. Att även den verksamheten har sin grund i passlagen framgår av 3 § tredje stycket passlagen och 6 § passförordningen

(1979:664). När utlandsmyndigheter utfärdar resehandlingar enligt utlänningslagstiftningen gäller utlänningsdatalagen (2016:27).

Utanför lagens tillämpningsområde faller sådan behandling av personuppgifter som utförs av andra än de angivna myndigheterna. Lagen gäller alltså inte när t.ex. Kriminalvården prövar en fråga om passstillstånd, när en socialnämnd yttrar sig över en passansökan eller när Migrationsverket genomför en passkontroll enligt passlagen. Lagen gäller inte heller när Polismyndigheten genomför en sådan kontroll, eftersom myndigheten då inte agerar som passmyndighet.

Lagen gäller vidare inte när Polismyndigheten behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Polismyndigheten agerar då inte som passmyndighet. Det är inte heller fråga om verksamhet enligt passlagen.

I *andra stycket* anges vilken slags behandling av personuppgifter som omfattas av lagens tillämpningsområde. Bestämmelserna i lagen ska endast tillämpas på behandling av personuppgifter som är helt eller delvis automatiserad eller på behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Vad som avses med register framgår av artikel 4.6 i dataskyddsförordningen.

Förhållandet till annan reglering

4 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Paragrafen anger lagens förhållande till dataskyddsförordningen. Övervägandena finns i avsnitt 6.4.

Av paragrafen framgår att lagen innehåller bestämmelser som kompletterar dataskyddsförordningen. Dataskyddsförordningen är direkt tillämplig i varje medlemsstat. Det innebär att den automatiskt är en del av den svenska rättsordningen. I vissa avseenden förutsätter eller tillåter dataskyddsförordningen emellertid att medlemsstaterna inför bestämmelser som kompletterar förordningen, antingen i form av preciseringar eller i form av undantag.

Denna lag innehåller bestämmelser som kompletterar dataskyddsförordningen när passmyndigheterna och Utrikesdepartementet behandlar personuppgifter i passverksamheten. De hänvisningar till dataskyddsförordningen som finns i lagen är dynamiska. Det innebär att hänvisningarna avser dataskyddsförordningen i dess vid varje tidpunkt gällande lydelse.

5 § Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Paragrafen anger lagens förhållande till lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och föreskrifter som har meddelats i anslutning till den lagen. Övervägandena finns i avsnitt 6.4.

Av paragrafen framgår att dataskyddslagen och föreskrifter som har meddelats i anslutning till dataskyddslagen gäller vid behandling av personuppgifter enligt passdatalagen. Detta gäller dock endast om ingenting annat följer av passdatalagen eller föreskrifter som har meddelats i anslutning till lagen.

Personuppgiftsansvar

6 § Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) är personuppgiftsansvariga för den behandling av personuppgifter som respektive myndighet utför.

Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i passregistret och passtillståndsregistret.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Övervägandena finns i avsnitt 6.5.

Personuppgiftsansvar innebär ett ansvar för att behandlingen av personuppgifter stämmer överens med dataskyddsförordningen och de kompletterande bestämmelser som finns i nationell rätt, bl.a. i denna lag. Det är till den personuppgiftsansvarige som den registrerade ska vända sig om han eller hon vill utöva sina rättigheter enligt regelverket, t.ex. begära rättelse av felaktiga personuppgifter.

Av *första stycket* framgår att passmyndigheterna och Regeringskansliet (Utrikesdepartementet) är personuppgiftsansvariga för den behandling av personuppgifter som respektive myndighet utför. Med detta menas att varje myndighet ansvarar för den personuppgiftsbehandling som sker inom ramen för myndighetens egen verksamhet. Om någon t.ex. har vänt sig till en ambassad med en ansökan om pass är ambassaden personuppgiftsansvarig för den behandling av personuppgifter som ambassaden utför när ansökan tas emot och ärendet handläggs. För uppgifter som därefter förs in i passregistret ansvarar Polismyndigheten enligt vad som anges i andra stycket.

Av *andra stycket* framgår att Polismyndigheten ensam är personuppgiftsansvarig för behandlingen av personuppgifter i passregistret och passstillståndsregistret. Bestämmelsen innebär att Polismyndigheten ansvarar för att behandlingen i dessa register överensstämmer med regelverket om dataskydd. Den som t.ex. vill begära rättelse av uppgifter i passregistret ska alltså vända sig till Polismyndigheten.

Ändamålen med behandlingen

7 § Personuppgifter får behandlas om det är nödvändigt för handläggning av ärenden om pass.

I paragrafen anges det primära ändamål som personuppgifter får behandlas för. Övervägandena finns i avsnitt 6.6.2.

Av paragrafen framgår att passmyndigheterna och Utrikesdepartementet får behandla personuppgifter om det är nödvändigt för handläggning av ärenden om pass. Det är fråga om ett primärt ändamål, dvs. ett ändamål för vilket de angivna myndigheterna både får samla in personuppgifter och behandla de uppgifter som har samlats in. De s.k. sekundära ändamål som regleras i 8–11 §§ medger endast behandling av personuppgifter som redan har samlats in.

Kravet på att behandlingen ska vara nödvändig för handläggning av passärenden innebär inte att behandlingen ska vara oundgänglig. Behandlingen kan anses nödvändig och därmed tillåten om den leder till effektivitetsvinster. Att behandlingen skulle kunna ske manuellt, utan tekniska hjälpmedel, hindrar normalt inte att en automatiserad behandling kan anses nödvändig (prop. 2017/18:105 s. 189).

Ändamålsbestämmelsen ger stöd för personuppgiftsbehandling i alla typer av passärenden. Det saknar alltså betydelse om ärendet i

det enskilda fallet gäller exempelvis utfärdande av pass, återkallelse av pass eller indragning av pass. Bestämmelsen ger vidare stöd för att behandla personuppgifter vid alla åtgärder som är nödvändiga att vidta i ärendet. Det kan handla om t.ex. mottagande, diarieföring, kommunicering eller läsning av personuppgifter, sökning efter personuppgifter, utfärdande av pass eller expediering av beslut.

Vilka personuppgifter som är nödvändiga att samla in i ärenden om pass framgår i första hand av bestämmelserna i passlagen (1978:302) och föreskrifter som har meddelats i anslutning till den lagen. Det förutsätts inte att en behandling är nödvändig för handläggningen av ett specifikt ärende för att den ska vara tillåten. Inom tillämpningsområdet faller även t.ex. mottagande av anmälningar från chefsöverläkare i enlighet med 20 § 1 passlagen. Uppgifterna i sådana anmälningar är nödvändiga att behandla för att det i ett senare skede ska kunna avgöras om det finns hinder mot att utfärda pass. Behandling kan även ske för planering, uppföljning och utvärdering av passverksamheten, eftersom detta anses vara en integrerad del av själva verksamheten (se t.ex. prop. 2014/15:148 s. 108).

8 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för gränskontroll.

Paragrafen reglerar ett sekundärt ändamål som personuppgifter får behandlas för. Övervägandena finns i avsnitt 6.6.3.

Av paragrafen framgår att personuppgifter som behandlas enligt 7 § även får behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för gränskontroll. Kravet på att behandlingen ska vara nödvändig innebär inte att den måste vara oundgänglig, se kommentaren till 7 §.

Bestämmelsen medger inte någon insamling av personuppgifter. Den tillåter bara att personuppgifter som redan har samlats in för handläggning av passärenden behandlas av Polismyndigheten för det ändamål som anges. Bestämmelsen ger inte övriga passmyndigheter eller Utrikesdepartementet stöd för att behandla personuppgifter.

Med gränskontroll avses kontroll av svenska och utländska medborgare som passerar Sveriges gränser eller Schengengränserna. Polismyndigheten har enligt 5 a § passlagen (1978:302) och 9 kap. 1 § utlänningslagen (2005:716) huvudansvaret för sådan kontroll.

Den personuppgiftsbehandling som förekommer vid gränskontroll omfattas inte i sig av passdatalagens tillämpningsområde. Däremot behöver Polismyndigheten kunna behandla de personuppgifter som finns i passverksamheten, inte minst i passregistret, för att kunna utföra gränskontrollen. Denna bestämmelse klargör att uppgifterna i passverksamheten får användas av myndigheten för detta ändamål.

I verksamheten med gränskontroll biträds Polismyndigheten av Tullverket, Kustbevakningen och Migrationsverket. Möjligheten för dessa myndigheter att ta del av personuppgifter i t.ex. passregistret regleras främst genom den sekundära ändamålsbestämmelsen i 10 § samt bestämmelserna i 22 och 23 §§ om uppgiftsskyldighet för Polismyndigheten och elektroniskt utlämnande av personuppgifter.

9 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

Paragrafen reglerar ett sekundärt ändamål som personuppgifter får behandlas för. Övervägandena finns i avsnitt 6.6.4.

Av paragrafen framgår att personuppgifter som behandlas enligt 7 § även får behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Kravet på att behandlingen ska vara nödvändig innebär inte att den måste vara oundgänglig, se kommentaren till 7 §.

Bestämmelsen medger inte någon insamling av personuppgifter. Den tillåter bara att personuppgifter som redan har samlats in för handläggning av passärenden behandlas av Polismyndigheten för de ändamål som anges. Bestämmelsen ger inte övriga passmyndigheter eller Utrikesdepartementet stöd för att behandla personuppgifter.

De ändamål som anges i paragrafen motsvarar de som anges i 1 kap. 1 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Vid den fortsatta behandlingen för dessa ändamål gäller den lagen och brottsdatalagen (2018:1177).

Vid sidan av Polismyndigheten har även andra myndigheter uppgifter som rör brottsbekämpning och lagföring. Möjligheten för dessa myndigheter att ta del av personuppgifter i t.ex. passregistret

regleras främst genom den sekundära ändamålsbestämmelsen i 10 § samt bestämmelserna i 21–23 och 25 §§ om uppgiftsskyldighet för Polismyndigheten och elektroniskt utlämnande av personuppgifter.

10 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Paragrafen reglerar ett sekundärt ändamål som personuppgifter får behandlas för. Övervägandena finns i avsnitt 6.6.5.

Av paragrafen framgår att personuppgifter som behandlas enligt 7 § även får behandlas om det är nödvändigt för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Kravet på att behandlingen ska vara nödvändig innebär inte att den måste vara oundgänglig, se kommentaren till 7 §. Bestämmelsen medger inte någon insamling av personuppgifter. Den tillåter bara att personuppgifter som redan har samlats in för handläggning av passärenden behandlas om det är nödvändigt för att lämna ut uppgifterna i överensstämmelse med lag eller förordning. Bestämmelsen kan tillämpas av alla passmyndigheter och av Utrikesdepartementet.

I vissa fall finns en uttrycklig skyldighet för passmyndigheterna eller Utrikesdepartementet att lämna ut uppgifter till enskilda eller till en myndighet, t.ex. enligt 21 och 22 §§ eller enligt 6 kap. 4 och 5 §§ offentlighets- och sekretesslagen (2009:400). I andra fall kan uppgiftslämnandet anses påbjudet eller önskvärt enligt författning, exempelvis på grund av myndigheternas allmänna serviceskyldighet gentemot enskilda (se t.ex. prop. 2017/18:113 s. 42).

11 § Personuppgifter som behandlas enligt 7 § får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Paragrafen reglerar övriga sekundära ändamål som personuppgifter får behandlas för. Övervägandena finns i avsnitt 6.6.6.

Av paragrafen framgår att personuppgifter som behandlas enligt 7 § även får behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket de samlades in. Bestämmelsen, som kan tillämpas av alla passmyndigheter och av Utrikesdepartementet, medger inte

någon insamling av personuppgifter. Den tillåter bara att personuppgifter som redan har samlats in för handläggning av passärenden behandlas för andra ändamål enligt den s.k. finalitetsprincipen.

Bestämmelsen är utformad i nära anslutning till artikel 5.1 b i dataskyddsförordningen och ska tolkas på samma sätt som den artikeln. Det innebär bl.a. att behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller vissa statistiska ändamål inte ska anses vara oförenlig med insamlingsändamålen. Det innebär också att de omständigheter som anges i artikel 6.4 a–e i förordningen ska beaktas vid bedömningen av om behandlingen är förenlig med insamlingsändamålen.

Rätten att göra invändningar

12 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

I paragrafen anges en begränsning av den registrerades rättigheter enligt dataskyddsförordningen. Övervägandena finns i avsnitt 6.7.

Paragrafen innebär ett undantag från den rätt att invända mot personuppgiftsbehandling som följer av artikel 21.1 i dataskyddsförordningen. Undantaget har stöd i artikel 23 i förordningen. Vid sådan behandling av personuppgifter som är tillåten enligt passdatalagen eller föreskrifter som har meddelats i anslutning till passdatalagen gäller inte rätten att göra invändningar enligt artikel 21.1.

Säkerhetsåtgärder

13 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

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

- 1. närmare föreskrifter om tillgången till personuppgifter, och*
- 2. ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.*

Paragrafen reglerar säkerhetsåtgärder till skydd för personuppgifter. Övervägandena finns i avsnitt 6.8.

Av *första stycket* framgår att tillgången till personuppgifter inom passmyndigheterna och Utrikesdepartementet ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter. Anställda och andra personer som deltar i verksamheten ska alltså inte ges tillgång till andra eller fler personuppgifter än vad som behövs med hänsyn till deras arbete. Det är respektive myndighet som i egenskap av personuppgiftsansvarig ansvarar för att avgöra vilka personuppgifter varje person behöver ha tillgång till för att kunna fullgöra sina arbetsuppgifter. Tillgången till personuppgifter kan begränsas genom tekniska och organisatoriska åtgärder.

Andra stycket innehåller en upplysningsbestämmelse. I den anges att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om tillgången till personuppgifter. Det som avses är verkställighetsföreskrifter. I bestämmelsen anges också att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter. Det finns alltså ett utrymme för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om andra säkerhetsåtgärder än den som framgår av första stycket.

Register i passverksamheten

14 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett passregister och ett passtillståndsregister.

Av paragrafen framgår att Polismyndigheten ska föra ett passregister och ett passtillståndsregister. Övervägandena finns i avsnitt 6.9.

En bestämmelse av samma innebörd finns för närvarande i 23 § första stycket passförordningen (1979:664). Beteckningen passtillståndsregister används dock inte i passförordningen.

Vad de två registren får innehålla regleras i 15 och 16 §§.

15 § Passregistret får endast innehålla uppgifter om en person som är eller har varit part i ett ärende om pass. Passregistret får i fråga om en sådan person endast innehålla följande uppgifter:

- 1. namn,*
- 2. person- eller samordningsnummer,*
- 3. medborgarskap,*
- 4. födelseort,*

5. kön,
6. längd,
7. ansiktsbilder som har tagits vid passansökningar,
8. biometriska uppgifter som har tagits fram ur ansiktsbilderna,
9. namnteckningar som har lämnats vid passansökningar,
10. uppgifter i handlingar som har kommit in eller upprättats, och
11. uppgifter om pass och om handläggningen av ärenden om pass.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter som får behandlas med stöd av första stycket.

Paragrafen reglerar innehållet i passregistret. Övervägandena finns i avsnitt 6.9 och 6.10.

I första stycket anges inledningsvis att passregistret endast får innehålla uppgifter om en person som är eller har varit part i ett ärende om pass. Part har samma innebörd som enligt förvaltningslagen (2017:900). Någon legaldefinition av ordet finns inte men det avser i regel den som är sökande, klagande eller annan part (jfr propositionen En modern och rättssäker förvaltning – ny förvaltningslag, prop. 2016/17:180 s. 79 f. och 294 f.). Det innebär att passregistret får innehålla uppgifter om den som har ansökt om pass, oavsett om pass har utfärdats eller inte. I båda fallen har personen varit part. Registret får också innehålla uppgifter om andra personer som är eller har varit parter i ärenden om pass, t.ex. efter överklagande eller vid återkallelse eller omhändertagande av ett pass. Registret får inte innehålla uppgifter om andra personer än de som räknas som parter.

I första stycket 1–11 anges vilka uppgifter registret får innehålla om den som är eller har varit part i ett ärende om pass. Uppräkningen är uttömmande. Andra uppgifter får alltså inte behandlas i registret. Med biometriska uppgifter i första stycket 8 avses detsamma som i artikel 4.14 i dataskyddsförordningen, dvs. personuppgifter som har erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter. Foton anses dock utgöra biometriska uppgifter endast när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person (skäl 51 till förordningen). Att både ansiktsbilder och de biometriska uppgifter som har tagits fram ur sådana bilder får

sparas i passregistret innebär att de biometriska uppgifterna kan sparas både självständigt och som en del av ansiktets bilden, genom att den sparas i ett sådant tekniskt format att biometriska jämförelser kan göras. Förutsättningarna för sökning i passregistret med hjälp av ansiktets bilder och biometriska uppgifter regleras i 19 §.

Andra stycket innehåller en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om vilka uppgifter som får behandlas med stöd av första stycket. Det som avses är verkställighetsföreskrifter.

16 § Passtillståndsregistret får endast innehålla de uppgifter som är nödvändiga för att man ska kunna avgöra om det krävs passtillstånd för en person enligt 20 § 1 eller 3 passlagen (1978:302).

Paragrafen reglerar innehållet i passtillståndsregistret. Övervägandena finns i avsnitt 6.9.

Passtillståndsregistret får enligt bestämmelsen endast innehålla de uppgifter som är nödvändiga för att man ska kunna avgöra om det krävs passtillstånd för en person enligt 20 § 1 eller 3 passlagen (1978:302). Vilka uppgifter som får behandlas i registret måste alltså bedömas utifrån de angivna bestämmelserna i passlagen. Det är normalt sett fråga om uppgifter om namn och personnummer liksom information om anmälningar från chefsöverläkare eller framställningar från Socialstyrelsen. Eftersom sådana uppgifter kan vara integritetskänsliga ställs särskilt höga krav på säkerheten i samband med behandlingen (artikel 32 i dataskyddsförordningen). Om någon begär att få ta del av uppgifter i registret måste en noggrann sekretessprövning göras. När passtillstånd inte längre krävs för en person enligt 20 § 1 eller 3 passlagen finns det inte längre stöd för att behandla uppgifter om personen i passtillståndsregistret. Detta följer både av paragrafens ordalydelse och av principen om lagringsminimering, se kommentaren till 26 §.

Behandling av känsliga personuppgifter

17 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas i följande fall:

1. i passregistret när det är tillåtet enligt 15 §,
2. i passstillståndsregistret när det är tillåtet enligt 16 §, och
3. vid sökning som är tillåten enligt 19 § andra stycket.

I paragrafen regleras när känsliga personuppgifter får behandlas. Övervägandena finns i avsnitt 6.10 och 6.11.

I *första stycket* anges att känsliga personuppgifter får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen. De kategorier av personuppgifter som avses är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening, genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste behovet av att behandla uppgifterna prövas noggrant i varje enskilt fall.

Regleringen i passlagen (1978:302) förutsätter att biometriska uppgifter och uppgifter om hälsa i viss utsträckning samlas in och behandlas för handläggning av passärenden. Detta är tillåtet enligt paragrafen, under förutsättning att behandlingen är absolut nödvändig för ändamålet. I vissa fall kan bestämmelserna i passlagen medföra att även uppgifter som avslöjar ras eller etniskt ursprung behandlas, eftersom en kombination av t.ex. ansiktsbild samt uppgifter om namn, medborgarskap och födelseort kan anses avslöja en persons ras eller etniska ursprung. Även sådan behandling är tillåten om den är absolut nödvändig för ändamålet.

Uppgifter som avslöjar politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening, genetiska uppgifter och uppgifter om en persons sexualliv eller sexuella läggning får i princip aldrig behandlas i passverksamheten. Sådana uppgifter är inte nödvändiga för att ärenden om pass ska kunna handläggas och får därför inte samlas in med stöd av 7 §. Om en enskild ändå lämnar sådana uppgifter till en passmyndighet eller Utrikesdepartementet får de behandlas bara på de sätt som är absolut nödvändiga.

Av *andra stycket* framgår att känsliga personuppgifter i vissa fall får behandlas utan någon prövning av om behandlingen är absolut nödvändig för ändamålet. Enligt *andra stycket 1 och 2* får känsliga personuppgifter alltid behandlas när det är tillåtet enligt 15 och 16 §§ om innehållet i passregistret och passstillståndsregistret. Av

dessa paragrafer följer bl.a. att passregistret får innehålla sådana biometriska uppgifter som har tagits fram ur ansiktsbilder och att passstillståndsregistret får innehålla uppgifter om hälsa, om det är nödvändigt för att man ska kunna avgöra om det krävs passstillstånd för en person enligt 20 § 1 eller 3 passlagen. Enligt *andra stycket 3* får känsliga personuppgifter alltid behandlas vid sökningar som är tillåtna enligt 19 § andra stycket, dvs. vid vissa sökningar i passregistret med hjälp av den ansiktsbild som tas i samband med en passansökan och de biometriska uppgifter som tas fram ur bilden.

Sökbegränsningar

18 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelse som avses i artikel 10 i EU:s dataskyddsförordning.

Paragrafen förbjuder sökningar i visst syfte. Övervägandena finns i avsnitt 6.11.

Enligt paragrafen är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelse som avses i artikel 10 i dataskyddsförordningen. Begränsningen gäller oavsett om en sökning utförs i passregistret eller bland andra uppgifter som behandlas enligt lagen. Vad känsliga personuppgifter är anges i kommentaren till 17 §. De uppgifter som avses i artikel 10 i dataskyddsförordningen är personuppgifter om fällande domar i brottmål och straffprocessuella tvångsmedel (prop. 2017/18:105 s. 38). Sökbegränsningen omfattar alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter som avses i artikel 10. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har ett visst etniskt ursprung eller har dömts för brott. Däremot hindrar bestämmelsen inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, exempelvis för att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård.

19 § Det är förbjudet att använda fingeravtryck och ansiktsbilder samt biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder som sökbegrepp.

Trots förbudet får den ansiktsbild som tas vid en passansökan och de biometriska uppgifter som tas fram ur ansiktsbilden användas vid sökning i passregistret, för att kontrollera sökandens identitet och innehav av pass i samband med passansökan.

Paragrafen begränsar möjligheten att använda vissa sökbegrepp. Övervägandena finns i avsnitt 6.10.4 och 6.11.

Första stycket innehåller ett förbud mot att använda fingeravtryck och ansiktsbilder, samt sådana biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder, som sökbegrepp inom passverksamheten. Förbudet gäller oavsett om en sökning utförs i passregistret eller bland andra uppgifter som behandlas enligt lagen.

En liknande bestämmelse finns för närvarande i 6 b § passlagen (1978:302). Förbudet i denna paragraf har emellertid ett bredare tillämpningsområde. Förbudet tar inte endast sikte på de fingeravtryck och den ansiktsbild som tas av sökanden i samband med en passansökan. Det träffar alla fingeravtryck och ansiktsbilder, samt biometriska uppgifter som har tagits fram ur fingeravtryck och ansiktsbilder, oavsett om dessa har tagits vid en passansökan eller i något annat sammanhang. Förbudet är absolut i den meningen att syftet med sökningen saknar betydelse. Eftersom sökförbudet är absolut får sådana sökningar som är otillåtna inte utföras ens för att tillmötesgå en begäran om utlämnande av allmän handling. Detta följer av 2 kap. 7 § tryckfrihetsförordningen. En sammanställning anses enligt den paragrafen inte förvarad hos myndigheten om den innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig.

I *andra stycket* finns ett undantag från förbudet. Den ansiktsbild som tas vid en passansökan får enligt bestämmelsen användas vid sökning i passregistret, för att kontrollera sökandens identitet och innehav av pass i samband med passansökan. Samma sak gäller de biometriska uppgifter som tas fram ur ansiktsbilden. Syftet med bestämmelsen är att den ansiktsbild som tas ska kunna användas för biometrisk jämförelse med de ansiktsbilder som finns i passregistret, för att kontrollera sökandens identitet och att sökanden inte redan har ett pass under en annan identitet. Undantaget gäller bara vid

sökning i samband med passansökan. Sökningen måste alltså göras innan pass har utfärdats eller ärendet annars har avslutats.

20 § Sökförbuden i 18 § och 19 § första stycket gäller även vid sökningar i passregistret och passtillståndsregistret för andra ändamål än handläggning av ärenden om pass.

Paragrafen förtydligar när de sökbegränsningarna som finns i lagen gäller. Övervägandena finns i avsnitt 6.11.

I paragrafen anges att sökförbuden i 18 § och 19 § första stycket gäller även vid sökningar i passregistret och passtillståndsregistret för andra ändamål än handläggning av ärenden om pass.

Bestämmelser om vilka sekundära ändamål personuppgifter får behandlas för finns i 8–11 §§. Vid behandling av personuppgifter för dessa sekundära ändamål kommer passdatalagen i många fall inte att gälla. Behandlingen kan i stället komma att omfattas av exempelvis brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Denna paragraf klargör att de sökförbud som finns i passdatalagen gäller även vid sådana sökningar i passregistret och passtillståndsregistret som utförs för sekundära ändamål. Bestämmelsen innebär t.ex. att en ansiktsbild inte får användas vid en sökning i passregistret som Polismyndigheten utför för att utreda ett brott.

Uppgiftsskyldighet

21 § En passmyndighet eller Regeringskansliet (Utrikesdepartementet) har vid direktåtkomst enligt 25 § första stycket rätt att ta del av personuppgifter som en annan passmyndighet eller Regeringskansliet (Utrikesdepartementet) behandlar.

Säkerhetspolisen har vid direktåtkomst enligt 25 § andra stycket rätt att ta del av personuppgifter som behandlas i passregistret.

I paragrafen regleras viss uppgiftsskyldighet för passmyndigheterna och Utrikesdepartementet. Övervägandena finns i avsnitt 6.13.

I första stycket anges att en passmyndighet eller Utrikesdepartementet vid direktåtkomst enligt 25 § första stycket har rätt att ta del av personuppgifter som en annan passmyndighet eller Utrikesdepar-

tementet behandlar. Bestämmelsen innebär att var och en av myndigheterna har rätt att vid direktåtkomst ta del av uppgifter som den utlämnande myndigheten behandlar. Rätten att ta del av uppgifter gäller oavsett om uppgifterna förekommer i t.ex. passregistret, passstillståndsregistret eller pågående ärenden. Det är fråga om en sådan uppgiftsskyldighet som enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen (2009:400) bryter den sekretess som kan gälla för uppgifterna hos den utlämnande myndigheten.

Andra stycket ger Säkerhetspolisen en motsvarande rätt att vid direktåtkomst ta del av uppgifter som behandlas i passregistret.

22 § Polismyndigheten ska på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen, Ekobrottsmyndigheten, en svensk ambassad, ett svenskt lönat konsulat, Försvarmakten, Kustbevakningen, Tullverket, Skatteverket eller Kronofogdemyndigheten.

I paragrafen regleras en skyldighet för Polismyndigheten att lämna ut uppgifter på annat sätt än genom direktåtkomst. Övervägandena finns i avsnitt 6.13.

Enligt bestämmelsen ska Polismyndigheten på begäran lämna ut ett fotografi av en enskild från passregistret till vissa myndigheter. Det är fråga om en sådan uppgiftsskyldighet som enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen (2009:400) bryter den sekretess som kan gälla hos Polismyndigheten för fotografierna i passregistret. En bestämmelse av samma innebörd finns för närvarande i 23 § andra stycket passförordningen (1979:664). Med lönat konsulat avses ett sådant karriärkonsulat som ofta kallas för generalkonsulat och som leds av en utsänd tjänsteman.

Elektroniskt utlämnande av personuppgifter

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

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 24 och 25 §§.

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt. Övervägandena finns i avsnitt 6.12.

Enligt *första stycket* får personuppgifter lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Det utlämnande som avses är bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller motsvarande.

Den lämplighetsprövning som föreskrivs ska göras i varje enskilt fall. Vid prövningen har det betydelse vem mottagaren är. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter elektroniskt till en annan myndighet (prop. 2014/15:148 s. 113). När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Ett elektroniskt utlämnande kan vara olämpligt om det på grund av personuppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet i förlängningen kan leda till integritetsrisker. Särskild försiktighet bör iakttas när det gäller utlämnande av fotografier. Vid prövningen bör även informationssäkerheten vägas in (prop. 2014/15:148 s. 114).

Om det kan antas att personuppgifterna kan komma att behandlas i strid med dataskyddsförordningen eller dataskyddslagen efter ett utlämnande gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). Uppgifterna får då inte lämnas ut vare sig elektroniskt eller på annat sätt, på grund av sekretessen.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran i större utsträckning än vad som behövs för att myndigheten ska kunna pröva om det finns hinder mot att handlingen lämnas ut. Det kan ha betydelse vid prövningen av om det är lämpligt att lämna ut en handling elektroniskt.

I *andra stycket* anges att elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 24 och 25 §§. Det innebär att passmyndigheterna och Utrikesdepartementet inte kan medge ytterligare direktåtkomst utöver vad som framgår av 24 och 25 §§, vare sig till andra myndigheter eller till enskilda.

Med direktåtkomst avses att någon har direkt tillgång till någon annans register eller databas och kan söka efter information på egen hand, dock utan att kunna påverka innehållet i registret eller databasen. Högsta förvaltningsdomstolen har i avgörandet HFD 2015 ref. 61 bedömt att direktåtkomst föreligger om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i nuvarande 2 kap. 6 § första stycket tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt

hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt.

24 § Uppgift om ett pass giltighet får lämnas ut genom direktåtkomst.

I paragrafen anges att uppgift om ett pass giltighet får lämnas ut genom direktåtkomst. Övervägandena finns i avsnitt 6.12.2.

Den enda uppgift som enligt bestämmelsen får lämnas ut genom direktåtkomst är uppgiften att ett visst pass är giltigt eller inte giltigt. Denna uppgift får å andra sidan lämnas ut till alla kategorier av mottagare. Bestämmelsen har utformats med förebild i 16 § lagen (2015:899) om identitetskort för folkbokförda i Sverige. Paragrafen ger passmyndigheterna och Utrikesdepartementet en möjlighet att medge direktåtkomst. Den innebär däremot inte att någon har rätt att få sådan åtkomst.

25 § Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) får medge varandra direktåtkomst till personuppgifter.

Säkerhetspolisen får medges direktåtkomst till personuppgifter i passregistret. I sådant fall gäller sökförbuden i 18 § och 19 § första stycket.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheten att medge direktåtkomst enligt första och andra styckena.

Paragrafen reglerar vilka myndigheter som får medges direktåtkomst till personuppgifter. Övervägandena finns i avsnitt 6.12.2.

Paragrafen ger passmyndigheterna och Utrikesdepartementet en möjlighet att medge vissa myndigheter direktåtkomst. Den innebär inte någon rätt för en annan myndighet att få sådan åtkomst. Möjligheten att medge direktåtkomst har inte sekretessbrytande verkan. Sekretessbrytande bestämmelser finns i 21 §.

Enligt *första stycket* får passmyndigheterna och Regeringskansliet (Utrikesdepartementet) medge varandra direktåtkomst till personuppgifter. Innebörden är att myndigheterna kan medge varandra ömsesidig direktåtkomst till alla personuppgifter som behandlas med stöd av lagen. Direktåtkomst kan alltså medges till uppgifter i t.ex. passregistret, passtillståndsregistret eller pågående ärenden.

I *andra stycket* anges att Säkerhetspolisen får medges direktåtkomst till personuppgifter i passregistret. Begränsningen till passregistret innebär att Säkerhetspolisen inte får medges direktåtkomst

till personuppgifter som behandlas i t.ex. passtillståndsregistret eller pågående ärenden. De sökförbud som finns i lagen gäller för Säkerhetspolisen om direktåtkomst medges.

I *tredje stycket* finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av möjligheten att medge direktåtkomst enligt första och andra styckena.

Bevarande och gallring

26 § Uppgifter och handlingar i passregistret ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades.

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

1. att uppgifter och handlingar får bevaras för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i första stycket, och

2. avskiljande och begränsningar av åtkomsten till uppgifter och handlingar som bevaras för sådana ändamål som anges i 1.

Paragrafen reglerar hur länge uppgifter och handlingar får bevaras i passregistret. Övervägandena finns i avsnitt 6.14.

Som utgångspunkt gäller principen om lagringsminimering i passverksamheten. Principen innebär att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Om personuppgifter behandlas enbart för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får de dock lagras under längre tid. Principen om lagringsminimering framgår av artikel 5.1 e i dataskyddsförordningen. Förevarande paragraf preciserar vad som gäller beträffande uppgifter och handlingar i passregistret.

I *första stycket* anges att uppgifter och handlingar i passregistret ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades. Med gallring avses detsamma som i arkivlagstiftningen, dvs. att uppgifter och handlingar på ett eller annat sätt förstörs eller raderas.

Gallringsfristen innebär att uppgifter eller handlingar aldrig får bevaras längre tid än tio år. Fristen bildar alltså den yttersta gränsen för bevarande. I den utsträckning det redan vid en tidigare tidpunkt står klart att vissa uppgifter eller handlingar saknar betydelse ska de gallras redan då. Det är upp till Polismyndigheten, som enligt 6 § är personuppgiftsansvarig, att bedöma hur länge olika kategorier av personuppgifter behöver bevaras inom ramen för tioårsfristen.

Utgångspunkten för beräkningen av gallringsfristen är när det ärende som uppgifterna eller handlingarna hänför sig till avslutades. Ett passärende avslutas vanligtvis genom att pass utfärdas. Det kan dock förekomma att ärenden avslutas även på andra sätt, exempelvis genom att en passansökan avslås eller återkallas. Gallringsfristen är utformad så att gallring ska ske senast tio år efter utgången av det kalenderår då ärendet avslutades. Den senaste tidpunkten för gallring kommer därmed alltid att infalla i samband med ett årsskifte.

Bestämmelsen innebär att samtliga uppgifter och handlingar som är hänförliga till ett visst ärende ska gallras senast när fristen löper ut. Vilka uppgifter passregistret får innehålla framgår av 15 §.

I *andra stycket* finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att uppgifter och handlingar får bevaras för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i första stycket. Regeringen eller den myndighet som regeringen bestämmer kan också meddela föreskrifter om att uppgifter och handlingar som bevaras för sådana ändamål ska avskiljas och att åtkomsten till dem ska begränsas. Med avskiljande menas att personuppgifterna tas bort från automatiserade uppgiftssamlingar eller system som används i den löpande verksamheten, t.ex. ärendehanteringssystem.

27 § De fingeravtryck som tas vid en passansökan och de biometriska uppgifter som tas fram ur fingeravtrycken ska omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.

Paragrafen anger hur länge fingeravtryck och biometriska uppgifter som kan tas fram ur fingeravtryck får bevaras. Övervägandena finns i avsnitt 6.14.

Enligt paragrafen ska de fingeravtryck som tas vid en passansökan och de biometriska uppgifter som tas fram ur dessa omedelbart

förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. En bestämmelse av samma innebörd finns för närvarande i 6 a § passlagen (1978:302). Bestämmelsen innebär att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa får behandlas automatiserat under handläggningen av passärendet. Sedan ärendet avslutats får uppgifterna emellertid inte sparas någon annanstans än i passet. Det finns alltså ingen möjlighet att bygga upp ett separat fingeravtrycksregister med hjälp av de fingeravtryck som lämnas i passärenden (prop. 2008/09:132 s. 16).

10.2 Förslaget till lag om ändring i passlagen (1978:302)

5 a § Polismyndigheten ska övervaka att bestämmelserna i 5 § följs.

Den som enligt 5 § ska medföra pass ska på begäran

1. överlämna passet till en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Kustbevakningen, Tullverket eller Migrationsverket, och

2. låta en befattningshavare enligt 1 ta passinnehavarens fingeravtryck och en bild i digitalt format av hans eller hennes ansikte för kontroll av att dessa motsvarar de fingeravtryck och den ansiktsbild som finns sparade i passet.

Den som enligt 5 § i stället medför ett identitetskort utfärdat av en passmyndighet ska på begäran

1. överlämna identitetskortet till en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Kustbevakningen, Tullverket eller Migrationsverket, och

2. låta en befattningshavare enligt 1 ta en bild i digitalt format av hans eller hennes ansikte för kontroll av att denna motsvarar den ansiktsbild som finns sparad i identitetskortet.

När en kontroll enligt andra stycket 2 eller tredje stycket 2 har genomförts, ska fingeravtrycken och ansiktsbilden samt de biometriska *uppgifter* som då har tagits fram omedelbart förstöras.

Paragrafen innehåller bestämmelser om kontroll av pass och identitetskort. Paragrafen behandlas i avsnitt 6.10.4.

Ändringen innebär endast att uttrycket biometriska data i *fjärde stycket* byts ut mot uttrycket biometriska uppgifter. Det är fråga om en anpassning till dataskyddsförordningens terminologi. Begreppet biometriska uppgifter definieras i artikel 4.14 i förordningen.

6 a § Fingeravtrycken och ansiktsbilden enligt 6 § andra stycket 1 ska sparas i ett lagringsmedium i passet.

Paragrafen innehåller vissa bestämmelser om de fingeravtryck och den ansiktsbild som tas vid en passansökan. Paragrafen behandlas i avsnitt 6.10.4 och 6.14.

Paragrafen ändras genom att *andra stycket* upphävs. Enligt det stycket har hittills gällt att fingeravtrycken och de biometriska data som tas fram ur dessa och ur ansiktsbilden omedelbart ska förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. I den del som gäller fingeravtrycken förs bestämmelsen oförändrad över till 27 § passdatalagen (2020:000). Fingeravtrycken och de biometriska uppgifter som tas fram ur dessa ska alltså även i fortsättningen omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. De biometriska uppgifter som har tagits fram ur ansiktsbilden ska däremot, till skillnad från i dag, få sparas i passregistret. Detta framgår av 15 § passdatalagen.

10.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

22 kap.

1 § Sekretess gäller för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs och uppgiften förekommer i verksamhet som avser

1. folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen, eller

2. förande av eller uttag ur sjömansregistret.

Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av *en fotografisk bild av den enskilde, och biometrisk uppgift som har tagits fram ur en sådan bild*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

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

Paragrafen reglerar sekretess vid folkbokföring och annan liknande registrering av befolkningen. Paragrafen behandlas i avsnitt 7.

Paragrafen ändras genom ett tillägg i *andra stycket*. Tillägget innebär att den presumtion för sekretess som gäller i fråga om en fotografisk bild av den enskilde utsträcks till att gälla även sådana biometriska uppgifter som har tagits fram ur bilden. Vad som avses med biometriska uppgifter framgår av artikel 4.14 i dataskyddsförordningen. Anledningen till ändringen är att passregistret enligt 15 § passdatalagen (2020:000) ska få innehålla både ansiktsbilder och biometriska uppgifter som har tagits fram ur ansiktsbilder.

Sammanfattning Ds 2015:44

Promemorian innehåller förslag till en lag om behandling av personuppgifter i passmyndigheternas och Utrikesdepartementets passverksamhet, en passdatalag. Syftet med lagen är att göra det möjligt för passmyndigheterna och Utrikesdepartementet att behandla personuppgifter på ett ändamålsenligt sätt i myndigheternas passverksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Målsättningen är att skapa en teknikneutral och flexibel lag som innehåller de bestämmelser som är av central betydelse för integritetsskyddet, däribland ändamålen med behandlingen och de begränsningar som ska gälla för behandling av vissa uppgifter. Kompletterande bestämmelser meddelas genom förordning eller föreskrifter. Lagförslaget reglerar behandlingen av personuppgifter i passmyndigheternas och Utrikesdepartementets passverksamhet. Med passverksamhet avses den verksamhet som passmyndigheterna och Utrikesdepartementet ansvarar för enligt passlagen. Den föreslagna lagen ska gälla utöver personuppgiftslagen (1998:204) och ska ersätta det fåtal särregler om personuppgiftsbehandling som finns i passlagen (1978:302) och passförordningen (1979:664).

Promemorian innehåller också förslag till en förordning om behandling av personuppgifter i passmyndigheternas verksamhet avseende nationella identitetskort. Den föreslagna förordningen ska ersätta de särregler om personuppgiftsbehandling som finns i förordningen (2005:661) om nationellt identitetskort. Förordningen ska gälla utöver personuppgiftslagen.

Författningsförslagen föreslås träda i kraft så snart som möjligt. Tidigaste tidpunkt för ikraftträdande torde vara sommaren 2016.

Författningsförslag i fråga om pass i Ds 2015:44

Förslag till passdatalag

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Denna lag gäller vid behandling av personuppgifter i passmyndigheternas och Regeringskansliets (Utrikesdepartementet) passverksamhet. Med passverksamhet avses den verksamhet som passmyndigheterna och Regeringskansliet (Utrikesdepartementet) ansvarar för enligt passlagen (1978:302).

Lagen gäller bara 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.

Lagens syfte

2 § Syftet med denna lag är att göra det möjligt för passmyndigheterna och Regeringskansliet (Utrikesdepartementet) att behandla personuppgifter på ett ändamålsenligt sätt i sin passverksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Förhållandet till passlagen

3 § I denna lag har termer och begrepp som också förekommer i passlagen (1978:302) samma betydelse som i den lagen.

Förhållandet till personuppgiftslagen

4 § Vid behandling av personuppgifter som omfattas av denna lag gäller personuppgiftslagen (1998:204), om inte annat följer av denna lag eller föreskrifter som har meddelats med stöd av den.

Personuppgiftsansvar

5 § Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i passregistret och registret över omständigheter som avses i 20 § 1 och 3 passlagen (1978:302).

Passmyndigheterna och Regeringskansliet (Utrikesdepartementet) är personuppgiftsansvariga för den behandling av personuppgifter som respektive myndighet i övrigt utför med stöd av denna lag eller föreskrifter som har meddelats med stöd av denna lag.

Ändamål med personuppgiftsbehandlingen

6 § Personuppgifter får behandlas om det behövs:

1. för att pröva ansökan om pass,
2. för att pröva framställning om återkallelse av pass, om provisorisk återkallelse av pass eller om begränsning i giltighet för pass,
3. för att utfärda, återkalla, dra in eller makulera pass,
4. för att omhänderta eller överlämna pass enligt 17 och 18 §§ passlagen (1978:302),
5. vid talan mot beslut i passärenden, samt
6. för att i övrigt fullgöra passmyndigheternas och Regeringskansliets (Utrikesdepartementet) uppgifter enligt passlagen (1978:302).

7 § Personuppgifter som behandlas för de ändamål som anges i 6 § får också behandlas för kontroll av identitetsuppgifter och uppgifter om pass vid gränskontroll. Sådana uppgifter får också behandlas i

Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet samt vid myndighetens upprätthållande av den allmänna ordningen och säkerheten.

8 § Personuppgifter som behandlas för de ändamål som anges i 6 § får också behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

9 § I fråga om behandling av personuppgifter för andra ändamål än vad som anges i 6-8 §§, gäller 9 § första stycket d och andra stycket personuppgiftslagen (1998:204).

Den enskildes inställning till personuppgiftsbehandlingen

10 § Behandling av personuppgifter som är tillåten enligt denna lag får utföras även om den registrerade motsätter sig behandlingen.

Register

11 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett passregister och ett register över omständigheter som avses i 20 § 1 och 3 passlagen (1978:302).

12 § Passregistret får endast innehålla de uppgifter om en person som behövs för de ändamål som anges i 6 §, och som avser:

- a) för – och efternamn,
- b) personnummer,
- c) kön,
- d) födelseort,
- e) längd,
- f) ansiktsbild och
- g) namnteckning.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om de ytterligare uppgifter som registret får innehålla.

13 § Registret över omständigheter som avses i 20 § 1 och 3 passlagen (1978:302) får endast innehålla de uppgifter om en person som

behövs för de ändamål som anges i 6 §, och som avser personnummer och för – och efternamn.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om de ytterligare uppgifter som registret får innehålla.

Särskilda kategorier av personuppgifter

14 § Personuppgifter som avslöjar ras eller etniskt ursprung eller rör hälsa får behandlas om uppgifterna är nödvändiga för handläggningen av ett ärende eller om uppgifterna har lämnats i ett ärende och de endast behandlas i löpande text.

Sökförbud

15 § Som sökbegrepp får inte användas uppgifter som avslöjar ras eller etniskt ursprung eller uppgifter som rör hälsa. Som sökbegrepp får inte heller användas uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Fingeravtrycken och ansiktsbilden enligt 6 § andra stycket 1 passlagen (1978:302) samt de biometriska data som kan tas fram ur dessa får inte användas vid sökning med hjälp av automatiserad behandling.

Första stycket gäller inte vid sökning i en viss handling eller i ett visst ärende.

Bevarande och gallring

16 § Uppgifter ska gallras så snart uppgiften inte längre behövs för något av de ändamål som den behandlas för.

Fingeravtrycken enligt 6 § andra stycket 1 passlagen (1978:302) och de biometriska data som tas fram ur dessa och ur ansiktsbilden enligt 6 § andra stycket 1 samma lag ska omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.

Uppgifter i registret över omständigheter som avses i 20 § 1 och 3 passlagen (1978:302) ska gallras senast

1. när den person som uppgifterna avser inte längre är intagen för vård enligt lagen (1991:1128) om psykiatrisk tvångsvård eller lagen (1991:1129) om rättspsykiatrisk vård eller

2. när en anmälan enligt 20 § 1 passlagen (1978:302) har återkallats.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att gallring enligt första stycket ska ske senast vid en viss tidpunkt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter att uppgifter får bevaras så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt för forskningens behov, även om föreskrifterna kommer att avvika från första stycket.

Tillgången till personuppgifter

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

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

Utlämnande av personuppgifter

18 § Polismyndigheten ska på begäran lämna ut ett fotografi av en enskild från passregistret till Säkerhetspolisen, Ekobrottsmyndigheten, svensk ambassad, svenskt lönat konsulat, Försvarsmakten, Kustbevakningen, Tullverket, Skatteverket och Kronofogdemyndigheten.

Utlämnande på medium för automatiserad behandling

19 § Om en personuppgift får lämnas ut, får det ske på medium för automatiserad behandling.

Rättelse och skadestånd

20 § Bestämmelserna i 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
 2. Bestämmelsen i 16 § första stycket behöver inte börja tillämpas förrän den ...

Förslag till passdataförordning

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av passdatalagen (201X:XX). De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

Register

2 § Passregistret får, utöver de personuppgifter som anges i 12 § passdatalagen (201X:XX), också innehålla uppgifter om en person som avser:

- a) ärendenummer,
- b) dag för utfärdandet av passet, passnummer och giltighetstid,
- c) beslut om att ansökan har avslagits eller passet har återkallats samt uppgift om vad som har utgjort grund för ett sådant beslut och
- d) beslut om att passet har spärrats eller makulerats samt uppgift om vad som utgjort grund för ett sådant beslut.

Tillgången till personuppgifter

3 § Polismyndigheten får, efter att ha gett Regeringskansliet tillfälle att yttra sig, meddela närmare föreskrifter om tillgången till personuppgifter i passverksamhet för personer som är verksamma inom myndigheten. Regeringskansliet får, efter att ha gett Polismyndigheten tillfälle att yttra sig, meddela motsvarande föreskrifter för passmyndigheterna utom riket och Utrikesdepartementet.

Bevarande och gallring

4 § Riksarkivet får meddela föreskrifter om att personuppgifter får bevaras så att rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens

behov tillgodoses, även om föreskrifterna kommer att avvika från bestämmelsen om gallring i 16 § första stycket passdatalagen (201X:XXX).

Intresset av att uppgifterna ska bevaras ska vägas mot behovet av skydd för den enskildes personliga integritet.

Övriga bestämmelser

5 § En passinnehavare har rätt att hos en passmyndighet kontrollera den information som har sparats i lagringsmediet i passet.

6 § Polismyndigheten får, efter att ha gett Regeringskansliet tillfälle att yttra sig, meddela de ytterligare föreskrifter som behövs för Polismyndighetens verkställighet av passdatalagen (201X:XX) och denna förordning. Regeringskansliet får, efter att ha gett Polismyndigheten tillfälle att yttra sig, meddela motsvarande föreskrifter för passmyndigheter utom riket och Utrikesdepartementet.

7 § Innan Polismyndigheten och Regeringskansliet meddelar föreskrifter med stöd av denna förordning, ska Datainspektionen ges tillfälle att yttra sig i frågor som berör särskilda risker för intrång i den personliga integriteten.

Denna förordning träder i kraft den

Förslag till lag om ändring i passlagen (1978:302)

Härigenom föreskrivs i fråga om passlagen (1978:302)

dels att 6 b § ska upphöra att gälla,

dels att 6 a § ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

6 a §⁸

Fingeravtrycken och ansiktsbilden enligt 6 § andra stycket 1 ska sparas i ett lagringsmedium i passet. *Fingeravtrycken och de biometriska data som tas fram ur dessa och ur ansiktsbilden ska omedelbart förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits.*

Fingeravtrycken och ansiktsbilden enligt 6 § andra stycket 1 ska sparas i ett lagringsmedium i passet.

Denna lag träder i kraft den

⁸ Senaste lydelse 2009:387.

Förslag till förordning om ändring i passförordningen (1979:664)

Härigenom föreskrivs i fråga om passförordningen (1979:664)

dels att 22 a och 23 §§ att ska upphöra att gälla,

dels att rubriken närmast 23 § ska utgå,

dels att 19 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 19 a §, av följande lydelse,

dels att det närmast före 23 a § ska införas en ny rubrik som ska lyda ”Reseförbud och anmälningsskyldighet m.m.”.

Nuvarande lydelse

Föreslagen lydelse

19 §⁹

Anmälan av chefsöverläkare enligt 20 § 1 passlagen (1978:302) ska göras till Polismyndigheten. Chefsöverläkaren ska återkalla anmälan om de omständigheter som har föranlett den inte längre finns.

Anmälan av chefsöverläkare enligt 20 § 1 passlagen (1978:302) ska göras till Polismyndigheten. Chefsöverläkaren ska återkalla anmälan om de omständigheter som har föranlett den inte längre finns. *Chefsöverläkaren ska underrätta Polismyndigheten när den person som anmälan avser inte längre bereds sådan vård som anges i 20 § passlagen (1978:302).*

19 a §

Har ett pass återkallats på grund av en framställning enligt 24 § andra stycket passlagen (1978:302) ska Socialstyrelsen underrätta Polismyndigheten när den person vars pass har återkallats inte längre bereds sådan vård som anges i 20 § passlagen (1978:302).

⁹ Senaste lydelse 2014:1130.

Denna förordning träder i kraft den

Förteckning över remissinstanserna (Ds 2015:44)

Remissvar har lämnats av Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Kustbevakningen, Migrationsverket, Datainspektionen, Sveriges ambassad London, Sveriges ambassad Washington, Forsvarsmakten, Socialstyrelsen, Tullverket, Skatteverket, Kronofogdemyndigheten, Riksarkivet, Sveriges advokatsamfund och Lunds universitet.

Riksdagens ombudsmän har avstått från att yttra sig.

Departementsserien 2019

Kronologisk förteckning

1. Straffrättsliga åtgärder mot tillgreppsbrott och vissa andra brott. Ju.
2. Höjda åldersgränser i pensionssystemet och i andra trygghetssystem. S.
3. Tydligare regler vid konsumentavtal. Ju.
4. Förslag till en nationell institution för mänskliga rättigheter i Sverige. Ku.
5. Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning. Ju.

Departementsserien 2019

Systematisk förteckning

Justitiedepartementet

Straffrättsliga åtgärder mot tillgrepsbrott
och vissa andra brott. [1]

Tydligare regler vid konsumentavtal. [3]

Passdatalag
– en ny lag som kompletterar
EU:s dataskyddsförordning. [5]

Kulturdepartementet

Förslag till en nationell institution för
mänskliga rättigheter i Sverige. [4]

Socialdepartementet

Höjda åldersgränser i pensionssystemet
och i andra trygghetssystem. [2]