Regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i polisens verksamhet, lag om genomförande av direktivet om användning av passagerar-uppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet samt till vissa lagar som har samband med dessa

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

Målet med propositionen är att uppdatera lagstiftningen om behandling av personuppgifter i polisens verksamhet så att den svarar mot de förändringar som skett i polisens nationella och internationella operativa miljö. I propositionen beaktas de ändringsbehov som följer av Europeiska unionens dataskyddsförordning och dataskyddsdirektiv. Vidare tas det hänsyn till vissa nationella behov av uppgiftsbehandling i synnerhet när det gäller polisens brottsbekämpning.

Genom propositionen genomförs också Europaparlamentets och rådets direktiv om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att bekämpa terroristbrott och grov brottslighet.

I syfte att säkerställa integritetsskyddet ska det föreskrivas om ändamålen med behandlingen av personuppgifter och förutsättningarna för att personuppgifter ska kunna överlåtas.

Ett annat mål med propositionen är att förtydliga och förenkla lagen, vars struktur blivit relativt svårtydd, och att på så sätt ge akt på de observationer som riksdagens förvaltningsutskott tidigare har gjort om lagen, inklusive att utveckla tillsynen över polisens personregister.

Lagarna avses träda i kraft så snart som möjligt.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL 1

ALLMÄN MOTIVERING 7

1 INLEDNING 7

2 NULÄGE 8

2.1 Lagstiftning 8

2.2 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU 17

2.3 Bedömning av nuläget 24

3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN 30

3.1 Målsättning 30

3.2 Alternativ 31

3.3 De viktigaste förslagen 34

4 PROPOSITIONENS KONSEKVENSER 38

4.1 Ekonomiska konsekvenser 38

4.2 Konsekvenser för samhällsekonomin och totalekonomiska konsekvenser 46

4.3 Konsekvenser för myndigheterna 47

4.4 Samhälleliga konsekvenser 60

5 BEREDNINGEN AV PROPOSITIONEN 67

5.1 Beredningsskeden och beredningsmaterial 67

5.2 Remissyttranden och hur de har beaktats 67

6 SAMBAND MED ANDRA PROPOSITIONER 67

DETALJMOTIVERING 70

1 LAGFÖRSLAG 70

1.1 Lag om behandling av personuppgifter i polisens verksamhet 70

1.2 Lag om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet 108

1.3 Lag om Enheten för grå ekonomi 123

1.4 Lag om kontrollavgift i kollektivtrafik 123

1.5 Lag om besöksförbud 123

1.6 Lag om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet 124

1.7 Lag om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor 124

1.8 Lag om brottsbekämpning inom Tullen 124

1.9 Lag om privata säkerhetstjänster 124

1.10 Lag om militär disciplin och brottsbekämpning inom försvarsmakten 124

1.11 Lag om behandling av personuppgifter inom Tullen 124

1.12 Tvångsmedelslag 124

1.13 Skjutvapenlagen 125

1.14 Lotterilagen 125

1.15 Lagen om nödcentralsverksamhet 125

1.16 Lag om utlänningsregistret 125

1.17 Utlänningslagen 126

1.18 Lagen om penninginsamlingar 126

1.19 Passlagen 126

1.20 Lagen om identitetskort 126

1.21 Lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet 127

1.22 Lagen om genomförande av vissa bestämmelser i beslutet om Eurojust 127

1.23 Lagen om verkställighet av böter.....127

1.24 Lagen om stark autentisering och betrodda elektroniska tjänster.....127

1.25 Polislagen.....127

1.26 Lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning.....128

1.27 Lagen om behandlingen av personer i förvar hos polisen 128

1.28 Lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet.....128

1.29 Säkerhetsutredningslagen.....129

1.30 Lagen om centralen för utredning av penningtvätt.....129

1.31 Lagen om förhindrande av penningtvätt och av finansiering av terrorism 130

1.32 Lagen om Polisyrkeshögskolan 130

1.33 Lagen om vittnesskyddsprogram.....130

2 NÄRMARE BESTÄMMELSER OCH FÖRESKRIFTER.....130

3 IKRAFTTRÄDANDE.....130

4 FÖRHÅLLANDE TILL GRUNDLAGEN SAMT LAGSTIFTNINGSORDNING.....131

4.1 Skyddet för privatlivet.....131

4.2 Jämlikhet.....144

4.3 Administrativa påföljder och ändringssökande 147

LAGFÖRSLAG 149

om behandling av personuppgifter i polisens verksamhet 149

om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.172

om ändring av 12 § i lagen om Enheten för utredning av grå ekonomi 179

om ändring av 6 § i lagen om kontrollavgift i kollektivtrafik 180

om ändring av 15 § i lagen om besöksförbud 181

om ändring av 17 § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet 182

om ändring av 9 § i lagen om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor 183

om ändring av 2 kap. 15 § i lagen om brottsbekämpning inom Tullen 184

om ändring av 86 § i lagen om privata säkerhetstjänster 185

om ändring av 42 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten ... 186

om ändring av 17 § i lagen om behandling av personuppgifter inom Tullen 187

om ändring av 9 kap. 4 § och 10 kap. 62 § i tvångsmedelslagen 188

om ändring av 113 § i skjutvapenlagen 189

om ändring av 42 b § i lotterilagen 190

om ändring av 17 och 19 § i lagen om nödcentralsverksamhet 191

om ändring av utlänningsregistret 192

om ändring av 131 § i utlänningslagen 194

om ändring av 27 § i lagen om penninginsamlingar 195

om ändring av 29 § i passlagen 196

om ändring av 17 och 31 § i lagen om identitetskort 197

om ändring av lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet 198

om ändring av lagen om genomförande av vissa bestämmelser i beslutet om Eurojust 200

om ändring av 1 och 19 § i lagen om verkställighet av böter 201

om ändring av 7 b § i lagen om stark autentisering och betrodda elektroniska tjänster 202

om ändring av 5 kap. 41 och 60 § i polislagen 203

om ändring av 5 § i lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning 204

om ändring av lagen om behandlingen av personer i förvar hos polisen 205

om ändring av 5 och 6 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet 207

om ändring av säkerhetsutredningslagen 208

om ändring av 3 och 4 § i lagen om centralen för utredning av penningvätt 210

om ändring av lagen om förhindrande av penningtvätt och av finansiering av terrorism 212

om ändring av 49 § i lagen om Polisyrkeshögskolan 214

om ändring av 13 § i lagen om vittnesskyddsprogram 215

ALLMÄN MOTIVERING

1 Inledning

Lagen om behandling av personuppgifter i polisens verksamhet (761/2003 rd, nedan polisväsendets personuppgiftslag) omarbetades i sin helhet år 2003. Lagen ersatte lagen om polisens personregister från år 1995 (509/1995 rd), dock så att den både strukturellt och innehållsmässigt i rätt stor utsträckning motsvarar lagen från år 1995.

I maj 2006 tillsattes ett lagstiftningsprojekt i syfte att se över polisväsendets personuppgiftslag. Arbetsgruppen hade i uppgift att granska lagen med beaktande av missförhållanden som uppdagats i den nationella tillämpningen, de ändringar som gjorts i lagstiftningen efter att lagen trätt i kraft samt den internationella utvecklingen. Arbetsgruppen färdigställde ett utkast till regeringsproposition i december 2009, varefter propositionen bereddes som ett tjänsteuppdrag vid inrikesministeriets polisavdelning. Regeringens proposition lämnades till riksdagen i juni 2010 (RP 98/2010 rd). Propositionen förföll i och med riksdagsvalet våren 2011.

Inrikesministeriets polisavdelning tillsatte i oktober 2011 ett lagstiftningsprojekt i syfte att utifrån den förfallna propositionen bereda en ändring av polisväsendets personuppgiftslag med hänsyn till de ändringsbehov som föranletts av att informationssystemet förnyats samt andra nödvändiga tekniska och strukturella ändringsbehov. Regeringens proposition (RP 66/2012 rd) med förslag till lagar om ändring av lagen om behandling av personuppgifter i polisens verksamhet och lagen om behandling av personuppgifter vid gränsbevakningsväsendet samt av vissa lagar som har samband med dem lämnades till riksdagen i juni 2012. Författningsändringarna trädde i kraft den 1 januari 2014.

Redan i samband med beredningen av regeringspropositionen (66/2012 rd) var det känt att lagen behövde omarbetas fullständigt. I motiveringstexten (s. 11) i regeringspropositionen konstateras att en totalreform av den gällande lagen skulle kräva en mer omfattande granskning och en utvärdering av lagstiftningstekniken i fråga om utlämnande och mottagande av uppgifter vid informationsutbyte mellan myndigheterna, och att en sådan granskning och utvärdering inte var möjlig att genomföra i samband med beredningen av propositionen.

I grundlagsutskottets utlåtande GrUU 18/2012 rd konstaterade utskottet att lagen bland annat som en följd av de många ändringar som gjorts i den har blivit mycket komplicerad till såväl struktur som innehåll. Lagen innehåller också ett flertal överlappningar med personuppgiftslagen och lagen om offentlighet i myndigheternas verksamhet. Utskottet anser att statsrådet har anledning att överväga en totalrevidering av lagen om behandling av personuppgifter i polisens verksamhet senast när det slutliga innehållet i den kommande EU-regleringen om dataskydd klarnar. I det sammanhanget blir det aktuellt exempelvis att ta in ett förbud mot etnisk profilering i lagstiftningen.

I riksdagens svar (RSv 2016/2013 rd) på regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om behandling av personuppgifter i polisens verksamhet och lagen om behandling av personuppgifter vid gränsbevakningsväsendet samt av vissa lagar som har samband med dem förutsatte riksdagen att regeringen snarast möjligt påbörjar en totalrevidering av polisväsendets personuppgiftslag och att man i samband därmed också beaktar dels det slutliga innehållet i den nya dataskyddslagstiftning som är under beredning i EU och vilka krav den ställer på den nationella lagstiftningen, dels de anmärkningar beträffande lagens struktur och innehåll som framgår av förvaltningsutskottets betänkande (FvUB 26/2013 rd), inklusive behovet av att utveckla tillsynen över de register som avses i polisväsendets personuppgiftslag. Riksdagen förutsatte dessutom att även bestämmelserna i lagen om behandling av personuppgifter vid gränsbevakningsväsendet ska justeras på samma gång. Förvaltningsut-

skottet konstaterar i sitt utlåtande att behovet av en totalrevidering av polisväsendets personuppgiftslag är uppenbart.

Inrikesministeriet tillsatte den 28 januari 2016 ett lagstiftningsprojekt i syfte att revidera polisväsendets personuppgiftslag. Arbetsgruppen hade i uppgift att sammanställa ett förslag till regeringsproposition med förslag till lag om behandling av personuppgifter i polisens verksamhet samt till vissa lagar som har samband med denna. Genom propositionen revideras den gällande lagen om behandling av personuppgifter i polisens verksamhet med beaktande av polisverksamhetens behov. I bestämmelserna beaktas de krav som ställs i Europeiska unionens dataskyddslagstiftning. Arbetsgruppens mandatperiod upphör den 28 februari 2018. Medlemmarna i arbetsgruppen representerar inrikesministeriets polisavdelning, inrikesministeriets gränsbevakningsavdelning, Polisstyrelsen, skyddspolisen, justitieministeriet, Brottspåföljdsmyndigheten, försvarsministeriet, huvudstaben, finansministeriet och Tullen. Därtill har dataombudsmannens byrå, centralkriminalpolisen och rättsregistercentralen utnämnt permanenta sakkunniga till arbetsgruppen.

Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan dataskyddsförordningen), Europaparlamentets och rådets direktiv (EU) 2016/680 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 (nedan dataskyddsdirektivet), samt Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (nedan PNR-direktivet) utfärdades den 27 april 2016.

Dataskyddsförordningen tillämpas från och med den 25 maj 2018. Medlemsstaterna ska utfärda och offentliggöra de lagar, förordningar och administrativa föreskrifter som är nödvändiga för att följa dataskyddsdirektivet senast den 6 maj 2018. De ska utan dröjsmål i skriftlig form informera kommissionen om dessa bestämmelser. Medlemsstaterna ska tillämpa dessa bestämmelser från och med den 6 maj 2018. Medlemsstaterna ska sätta i kraft de lagar, förordningar och administrativa föreskrifter som är nödvändiga för att följa PNR-direktivet senast den 25 maj 2018. De ska utan dröjsmål informera kommissionen om detta.

2 Nuläge

2.1 Lagstiftning

Eftersom det föreslås att lagen om behandling av personuppgifter i polisens verksamhet ska revideras som helhet till både innehåll och struktur beskrivs de gällande bestämmelserna i detta avsnitt endast på allmän nivå. Den gällande lagen innehåller bland annat detaljerade registerspecifika innehållsförteckningar, undantag från det huvudsakliga ändamålet med uppgifterna och tidsfrister för utplåning av uppgifter. Det är inte ändamålsenligt att redogöra närmare för dessa i detta sammanhang. Vidare har det föreskrivits tämligen detaljerat om utlämnandet av uppgifter mellan myndigheter och om rätten att få uppgifter. Avsnittet om bedömningen av nuläget tar upp missförhållanden som upptäckts i den gällande lagens paragrafer, orsakerna bakom dessa och motiveringar till förslaget att revidera lagen som helhet.

Allmänt

I 10 § 1 mom. i grundlagen konstateras att närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Enligt grundlagsutskottets vedertagna praxis begränsas lagstiftarens

spelrum förutom av denna bestämmelse även av att skyddet för personuppgifter delvis ingår i skyddet för privatlivet i samma moment. Lagstiftaren ska trygga denna rättighet på ett sätt som kan anses godtagbart med hänsyn till de grundläggande fri- och rättigheterna som helhet. Grundlagsutskottet har i sin praxis ansett att det är viktigt med tanke på skyddet för personuppgifter att reglera åtminstone registreringens syfte, innehållet i de registrerade personuppgifterna och tillåtna användningsändamål, vilket inbegriper uppgifternas överlåtbarhet och bevaringstiden för uppgifterna i personregistren, samt den registrerades rättsskydd. Regleringen av dessa faktorer på lagnivå ska dessutom vara omfattande och detaljerad. Enligt grundlagsutskottets avgörandepraxis kan dessa aspekter tillämpas på regleringen av användningen av personuppgifter även ur ett mer allmänt perspektiv.

Polisväsendets personuppgiftslag är en speciallag i förhållande till lagen om offentlighet i myndigheternas verksamhet (621/1999) och personuppgiftslagen (523/1999). I lagen föreskrivs om innehållet i de personuppgifter som ingår i polisens informationssystem och om principerna för behandlingen av uppgifterna.

1 kap.

Tillämpningsområde

I detta kapitel föreskrivs om lagens tillämpningsområde. Lagen tillämpas på automatisk behandling av personuppgifter som behövs för skötseln av de uppgifter som avses i 1 kap. 1 § i polislagen (872/2011) och på annan behandling av personuppgifter, då de utgör eller är avsedda att utgöra ett personregister eller en del av ett sådant.

Enligt 1 kap. 1 § i polislagen är det polisens uppgift att trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska upprätthålla säkerheten i samarbete med andra myndigheter samt med sammanslutningar och invånarna och sköta det internationella samarbete som hör till dess uppgifter. Enligt 1 kap. 1 § 2 mom. i polislagen ska polisen dessutom sköta uppgifter i samband med tillståndsförvaltningen och andra uppgifter som uttryckligen föreskrivs i lag samt inom ramen för sina uppgifter ge var och en den hjälp som han eller hon behöver. Om det finns grundad anledning att anta att en person har försvunnit eller råkat ut för en olycka ska polisen vidta de åtgärder som behövs för att finna personen. Polislagens 1 kap. 1 § 3 mom. innehåller hänvisningar till förundersökningslagen (805/2011), där det föreskrivs om förundersökning av brott, och till tvångsmedelslagen (806/2011), som innehåller bestämmelser om tvångsmedel som kan användas i förundersökningen av brott.

På polisens personregister och behandlingen av personuppgifter i polisens verksamhet tillämpas i andra hand den allmänna personuppgiftslagen (523/1999). På myndigheters behandling av personuppgifter tillämpas som en allmän lag även lagen om offentlighet i myndigheternas verksamhet (621/1999, offentlighetslagen). Offentlighetslagens bestämmelser om sekretess är relevanta vid behandlingen av personuppgifter. Med stöd av offentlighetslagen fastställs också en parts rätt att ta del av en handling. I 1 § i polisväsendets personuppgiftslag finns en informativ hänvisning till en subsidiär tillämpning av de två allmänna lagarna. I paragrafen hänvisas av informativa skäl även till internationella avtal som är bindande för Finland. Exempel på sådana avtal är konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter och Schengenkonventionen.

2 kap.

Allmänt

Polisens informationssystemshelhet består av polisens egna riksomfattande och enhetsspecifika informationssystem, statsförvaltningens gemensamma informationssystem som polisen använder samt andra myndigheters nationella och internationella informationssystem. Därtill använder polisen andra informationssystem som tillhandahålls av intressentgrupper. (Polisstyrelsens anvisning POL-2016-10558 om införande av datasystem och hantering av datasystemens livscykel vid polisen).

Lagens 2 kapitel innehåller bestämmelser om polisens riksomfattande informationssystem, den personuppgiftsansvarige och inrättande av riksomfattande och enhetsspecifika personregister. Kapitlets 9 § innehåller dessutom beträffande det nödcentralsdatasystem som polisen använder en hänvisningsbestämmelse till lagen om nödcentralsverksamhet (692/2010) och beträffande utlänningsregistret en hänvisningsbestämmelse till lagen om utlänningsregistret (1270/1997).

Polisen använder sig av flera personregister där man samlar känsliga eller sekretessbelagda uppgifter, och med tanke på polisens verksamhet och medborgarnas rättsskydd är det viktigt att dessa skyddas. De informationssystem som polisen använder är från olika tidsperioder och bygger på olika tekniska lösningar. Informationssystemen skyddas med olika säkerhetsmekanismer, som förvaltas som helhet via de olika delområdena av informationssäkerheten. Säkerheten är en ständig process, vars kontroll grundar sig på en enhetlig politik, principer om informationssäkerhet och anvisningar som baserar sig på dessa.

I den gällande personuppgiftslagen för polisväsendet föreskrivs om de informationssystem som används i polisens internationella samarbete. Många speciallagar som gäller polisens verksamhetsområde innehåller dessutom bestämmelser om enskilda personregister som polisen använder eller om skyldigheten att administrera filer som innehåller personuppgifter. Denna typ av registerspecifika bestämmelser finns exempelvis i lagen om centralen för utredning av penningtvätt (445/2017), som föreskriver om penningtvättsregistret, i lagen om vittnesskyddsprogram (88/2015), som föreskriver om registret över vittnesskyddsprogram, i passlagen (671/2006), som föreskriver om passregistret, samt i skjutvapenlagen (1/1998), som föreskriver om polisens skyldighet att föra sådana register som behövs för skötseln av tillstånds- och tillsynsuppgifterna. Dessutom innehåller lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009, nedan PTG-lagen) bestämmelser om behandlingen av uppgifter i ett så kallat tillfälligt register för brottsanalys, som var och en av dessa samarbetsmyndigheter kan inrätta med stöd av sin specifika speciallagstiftning om behandling av personuppgifter.

Informationssystemet för polisärenden

Informationssystemet för polisärenden är ett riksomfattande informationssystem som inrättats för att polisen ska kunna utföra de uppgifter som anges i 1 kap. 1 § 1 mom. i polislagen (872/2011). Bestämmelser om informationssystemet för polisärenden finns i 2 § i polisväsendets personuppgiftslag. Bland undersöknings- och handräckningsuppgifterna i informationssystemet för polisärenden antecknas bl.a. anmälningar som gjorts till polisen och de åtgärder som vidtagits till följd av en anmälan. Tröskeln för mottagande av anmälningar är låg. När någon anmäler ett brott eller en händelse som han eller hon misstänker vara ett brott till en förundersökningsmyndighet, ska myndigheten registrera anmälan utan dröjsmål. Om anmälan är oklar eller bristfällig ska den som gjort anmälan vid behov uppmanas att precisera eller komplettera den (förundersökningslagen, 3 kap. 1 §). Förutom anmälningar om brott registreras

bl.a. handräcknings-, polisundersöknings- och utlänningsärenden i systemet. Med polisundersökning avses annan undersökning som polisen enligt lag ska företa än förundersökning med anledning av brott.

Informationssystemet för polisärenden utgörs av olika typer av information. Utgående från användarnas behov har flera olika kategorier skapats för användningen av dessa. Användarrättigheterna består av flera olika användarroller, och ju fler roller användaren har desto mer omfattande är användarrättigheterna. Användarna ansöker om och beviljas rättigheter enligt arbetsuppgifter, behov och särskild ansökan. Lagtekniskt sett har de förteckningar över uppgifternas innehåll som ska registreras i systemet utformats så att de är uttömmande på det sätt som förutsätts i riksdagens utskottsutlåtande och utskottsbetänkande (GrUU 18/2012 rd och FvUB 26/2013 rd).

I den lagändring som trädde i kraft 2014 justerades bestämmelserna om informationsinnehåll som ska registreras i informationssystemet till vissa delar så att de motsvarade de funktionella behoven. En annan betydande ändring var att en ny bestämmelse om lagring av observationsuppgifter, 2 § 11 punkten, fogades till lagen. Med stöd av 11 punkten kan man i informationssystemet för polisärenden lagra uppgifter om observationer som gjorts av poliser eller uppgifter som anmälts till polisen i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser eller uppträdande i övrigt med fog kan bedömas ha samband med brottslig verksamhet. Villkoren för lagring i informationssystemet är lägre i fråga om dessa observationsuppgifter än i fråga om de uppgifter som ska lagras om misstänkta och som behandlas nedan i avsnittet Bedömning av nuläget. Grundlagsutskottet ansåg i sitt utlåtande (GrUU 22/2012 rd) att när regleringen begränsas på detta sätt i fråga om informationsinnehåll, användningsändamål och förvaringstid blir den inte problematisk med avseende på skyddet för personuppgifter. Med tanke på observationsuppgifternas karaktär är det emellertid viktigt att villkoren för lagring av uppgifter tolkas snävt och framför allt så att en observationsuppgift endast kan lagras om det finns en misstanke om brottslig verksamhet. Vidare ska strävan vara att uppgifterna ska granskas i den mån det är möjligt, och en bedömning av uppgifternas tillförlitlighet och riktighet ska fogas till uppgifterna alltid när det är möjligt.

Totalreformen av polisens system för verksamhetsstyrning, det s.k. Vitja-projektet, förenhetligar och effektiviserar polisens och de övriga säkerhetsmyndigheternas och rättsliga myndigheternas operativa informationssystem. Målet med systemet är att harmonisera förundersökningsmyndigheternas arbetsprocesser och att förnya och slå samman polisens nuvarande operativa system till en ur användarens synvinkel enhetlig och informationssäker systemhelhet. Även den registrerades rättsskydd beaktas i och med den enhetliga registreringsplattformen. Det nya informationssystemet används förutom av polisen även av de övriga förundersökningsmyndigheterna i Finland: Tullen, Gränsbevakningsväsendet och Försvarsmakten. Utöver dessa finns det flera myndigheter som använder systemet genom förfrågningar. I januari 2014 lanserades den första fasen av Vitja-systemet. Beslut om den andra lanseringsfasen fattas separat.

Antal användare av det nuvarande informationssystemet för polisärenden som övergår till Vitja-systemet, indelade efter användarorganisation (läget i oktober 2015):

Polisen	11 568
Tullen	1 293
Gränsbevakningsväsendet	2 142

Försvarsmakten - brottmål	69
Försvarsmakten - militär disciplin (ny)	2 500
Rättsregistercentralen (förfrågningar)	1
Fångvården (förfrågningar)	158
Brottspåföljdsmyndigheten (förfrågningar)	3
Utlänningsverket (förfrågningar)	146
Nödcentralsverket (förfrågningar)	533
Åklagarväsendet (undersökning av polisbrott, förfrågningar)	559
Sammanlagt	18 971

Informationssystemet för förvaltningsärenden

Informationssystemet för förvaltningsärenden är ett riksomfattande personregister som inrättats för att polisen ska kunna utföra de uppgifter som anges i 1 kap. 1 § 2 mom. i polislagen (872/2011). Bestämmelser om de uppgifter som ska lagras i informationssystemet finns i gällande 3 § i polisväsendets personuppgiftslag. I likhet med informationssystemet för polisärenden utgörs även innehållet i informationssystemet för förvaltningsärenden av olika typer av information. I 3 § finns en uttömmande förteckning över de uppgifter som ska registreras i systemet på det sätt som förutsätts i riksdagens utskottsutlåtande och utskottsbetänkande (GrUU 18/2012 rd och FvUB 26/2013 rd). Uppgifterna i informationssystemet för förvaltningsärenden lagras i flera olika registerapplikationer, för vilka användarrättigheter beviljas på ansökan på grundval av arbetsuppgifterna. Flera av registerapplikationerna i informationssystemet för förvaltningsärenden har förnyats under de senaste åren, och för närvarande håller man på att upphandla ett nytt vapeninformationssystem. Målet är att den första fasen av systemet ska införas 2018.

Förteckningen över de informationsinnehåll som ska lagras i informationssystemet för förvaltningsärenden har i flera etapper justerats för att svara mot de förändringar som skett i polisens tillståndsförvaltningsuppgifter. I samband med den lagändring som trädde i kraft i början av 2014 uppdaterades förteckningen över sådana grundläggande uppgifter som gäller en persons identitet och som ska lagras i systemet, och till förteckningen över uppgifter om vapentillstånd i 3 § 3 mom. 1 punkten fogades som en ny uppgift tidpunkten för lämplighetstestet för vapentillstånd. Till 3 mom. fogades dessutom en ny 8 punkt om lagring av uppgifter för tillsynen över penninginsamlingar och en ny 9 punkt om lagring av uppgifter om lotteritillstånd. Andra betydande ändringar som kan nämnas är att en ny punkt 4, som gäller fingeravtrycksuppgifter i pass, fogades till momentet år 2014, att uppgifterna om vapentillstånd kompletterades med uppgifterna i en sådan skjutvapenanmälan som avses i 114 § i skjutvapenlagen (1/1998) år 2015, och att 5 punkten, som gällde lagring av uppgifter om säkerhetsutredningar som görs av den lokala polisen, upphävdes år 2015 i samband med att den nya säkerhetsutredningslagen (726/2014) stiftades.

Förutom säkerhetsutredningarna har också körtillståndsärendena och utlänningsärendena överförts på andra myndigheter medan polisen koncentrerar sig på tillståndsärenden som är viktigare med tanke på den allmänna ordningen och säkerheten. Dessa ändringar har emellertid

inte påverkat polisväsendets personuppgiftslag, eftersom de personuppgifter som gäller tillstånden i fråga inte har lagrats i polisens informationssystem för förvaltningsärenden. Det totala antalet tillståndsärenden som polisen behandlade år 2016 var cirka 20 procent lägre jämfört med året innan, vilket beror på att de tillståndsärenden som enligt lag hör till polisens ansvar har minskat. Antalet behandlade tillståndsärenden som gäller resehandlingar har emellertid ökat.

Tillståndsärenden som behandlas av polisen, enligt tillståndskategori			
	2014	**2015**	**2016**
Resedokument sammanlagt	857 267	915 795	1 004 866
Pass	721 794	774 570	847 972
Identitetskort	135 473	141 225	156 894
Vapentillstånd	55 432	57 939	56 698
Tillstånd inom säkerhetsbranschen	56 841	60 771	26 738
Övriga ärenden	12 021	11 868	16 283
Utlänningstillstånd (från 1.1.2017 Migri)	*55 043*	*54 900*	*54 129*
Körtillstånd (från 1.1.2016 Trafi)	*355 524*	*350 977*	*1 442*
Samtliga tillstånd som beviljas av polisen	**1 392 128**	**1 452 250**	**1 160 156**

Informationssystemet för misstänkta

Bestämmelser om informationssystemet för misstänkta finns i 4 § i den gällande lagen. I informationssystemet kan registreras information som för skötseln av uppgifter enligt polislagen inhämtats genom kriminalunderrättelseverksamhet, observation eller iakttagelser och som gäller personer som skäligen kan misstänkas göra eller ha gjort sig skyldiga till ett brott på vilket kan följa fängelse, eller medverka eller ha medverkat till ett brott på vilket kan följa fängelse i mer än sex månader, eller till straffbart bruk av narkotika. Endast polispersonal som förordnats till kriminalunderrättelse-, brottsanalys- och observationsuppgifter samt de kontaktpersoner som polisen sänt utomlands har genom teknisk anslutning tillgång till informationssystemet för misstänkta. Med stöd av lagens 45 § 1 mom. gäller de registrerades rätt till insyn inte uppgifterna i informationssystemet för misstänkta.

För tillfället innehåller informationssystemet för misstänkta uppgifter om cirka 50 000 personer, av vilka de flesta har antecknats i systemet som misstänkta för brott och resten som misstänkta för medverkan till brott. Polisstyrelsen har med stöd av 4 § polisförvaltningslagen (110/1992) och polisväsendets personuppgiftslag utfärdat en anvisning om behandlingen av uppgifter som gäller informationssystemet för misstänkta (POL-2016-18786). Anvisningen är offentlig och gäller 1.4.2017–31.3.2021. Informationssystemet för misstänkta behandlas i detalj i avsnittet om tillsynen över personregister och bedömningen av nuläget.

Gränsbevakningsväsendet har i sitt funktionella datasystem till sitt förfogande ett undersöknings- och handräckningsregister som motsvarar informationssystemet för misstänkta, och Tullen på motsvarande sätt ett underrättelseregister.

Skyddspolisens funktionella informationssystem

Enligt 10 § i polisförvaltningslagen (110/1992) har skyddspolisen till uppgift att bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet samt att utföra undersökning av sådana brott. Skyddspolisen ska även upprätthålla och utveckla en allmän beredskap för att förebygga verksamhet som äventyrar rikets säkerhet.

Bestämmelser om skyddspolisens funktionella informationssystem finns i 5 § i polisväsendets personuppgiftslag. Personuppgifter som skyddspolisen behandlar förs in i informationssystemet, om lagringen av uppgifter uppfyller de villkor som anges i lagen. Det ska enligt 5 § vara fråga om uppgifter som behövs för att förebygga och utreda förehavanden eller brott som äventyrar rätts- och samhällsordningen eller statens säkerhet. Paragrafen innehåller en uttömmande förteckning över uppgifter som gäller en persons identitet på det sätt som förutsätts i riksdagens utskottsutlåtande och utskottsbetänkande (GrUU 18/2012 rd och FvUB 26/2013 rd).

Den personuppgiftsansvarige för skyddspolisens funktionella informationssystem är skyddspolisen. Skyddspolisen är också personuppgiftsansvarig för registret över säkerhetsutredningar. Separata bestämmelser om registret över säkerhetsutredningar finns i säkerhetsutredningslagen (726/2014).

Skyddspolisen kan med stöd av lagens 10 § behandla känsliga uppgifter som är nödvändiga för att skyddspolisen ska kunna utföra sitt uppdrag. Uppgifter som kan vara av betydelse med avseende på uppdragens karaktär och utförandet av dem kan vara uppgifter om en persons samhälleliga eller politiska uppfattning eller religiösa övertygelse.

Polisens övriga personregister

Bestämmelser om polisens övriga personregister finns i 6 § i polisväsendets personuppgiftslag. Med stöd av paragrafens 1 mom. kan det förutom de permanenta riksomfattande informationssystem som förs med hjälp av automatisk databehandling finnas temporära eller manuella personregister för polisens bruk.

Med stöd av 2 mom. kan det även inrättas andra personregister avsedda för en eller flera polisenheters bruk. Enligt 2 mom. 2 punkten är det bl.a. möjligt att inrätta ett temporärt register för sådan brottsanalys som behövs för att förhindra, avslöja eller utreda ett sådant brott eller en brottshelhet bestående av sådana brott som kan leda till fängelse, i vilket får samköras, lagras och annars behandlas uppgifter i de informationssystem som avses i 2–4 §, uppgifter som i samband med utförandet av ett enskilt polisuppdrag har inhämtats genom kriminalunderrättelseverksamhet, observation eller iakttagelser, samt uppgifter som avses i 14 § 1 mom. 2 och 4 punkten. Bestämmelsen ändrades genom den lag som trädde i kraft den 1 januari 2014 så att det blev möjligt att inrätta ett temporärt register för sådan brottsanalys som behövs för att förhindra, avslöja eller utreda förutom ett enskilt brott även en helhet bestående av flera brott. Denna ändring har effektiviserat utredningen av lokala, grova brott och i synnerhet omfattande brottsserier.

I avsnittet om bedömningen av nuläget behandlas i detalj vilka funktionella behov det finns inom polisverksamheten när det gäller behandlingen av uppgifter i anslutning till brottsanalys.

3 kap.

Kapitlet innehåller specialbestämmelser om behandling av personuppgifter. I kapitlets 10 § föreskrivs om ett undantag till förbudet att behandla känsliga uppgifter enligt 11 § i personuppgiftslagen. Bestämmelser om skydd av identifieringsuppgifter som grundar sig på fysiska egenskaper finns i 10 a §. Paragrafen fogades till lagen i samband med en ändring i passlagen, eftersom det då ansågs att införandet av biometriska identifieringsuppgifter (fingeravtryck) i ett register uttryckligen förutsatte att kraven på informationssäkerhet beaktas i lagstiftningen.

I lagens 11 § föreskrivs om behandling av överskottsinformation som erhållits med hemliga informationsinhämtningsmetoder. Genom den lagändring som trädde i kraft år 2014 preciserades grunderna för registrering av uppgifter, och det fastställdes i detalj i vilka register uppgifter får lagras. När det gäller användning av överskottsinformation hänvisas det i 11 § 2 mom. till paragraferna i polislagen och tvångsmedelslagen. Ur perspektivet för den myndighet som tillämpar lagen är det viktigt att grunderna för registreringen av uppgifter är enhetliga oberoende av om uppgifterna har inhämtats på de grunder som fastställs i polis- eller tvångsmedelslagen eller med vilken hemlig informationsinhämtningsmetod uppgifterna i praktiken har inhämtats. Observerade missförhållanden i behandlingen av överskottsinformation behandlas närmare i avsnittet Bedömning av nuläget.

I 12 § föreskrivs om behandling av uppgifter som inte hänför sig till ett visst uppdrag och i 13 § föreskrivs om polisens rätt att få uppgifter ur vissa register. På grund av lagändringar bygger systematiken i 13 § dels på hänvisningar till olika lagar, dels på föreskrifter om för vilka ändamål polisen har rätt att få uppgifter. Eftersom polisens informationssystem också används av många andra myndigheter har det varit nödvändigt att i 14 § föreskriva om uppgifter som andra myndigheter lämnar ut till polisen genom registrering vid direkt anslutning eller för registrering som en datamängd. Observerade missförhållanden i regleringen av rättigheten att få uppgifter och utlämnande av uppgifter behandlas närmare nedan i samband med bedömningen av nuläget.

4 kap.

I detta kapitel föreskrivs om användning och utlämnande av uppgifter ur polisens personregister. Enligt 15 § är det möjligt att använda uppgifter för det ändamål som uppgifterna har samlats in och registrerats för. De riksomfattande personregistren får användas av alla polisenheter, med undantag av Polisyrkeshögskolan. Ett enhetsspecifikt register får endast användas av de polisenheter som det inrättats för. Uppgifter kan under vissa i 16 § angivna förutsättningar också användas för andra ändamål än de som uppgifterna samlats in och registrerats för. I bestämmelserna om användning av uppgifter iakttas den förpliktande principen om ändamålsbegränsning som fastställs i 2 kap. 7 § i den allmänna personuppgiftslagen.

I samband med revideringen av passlagen år 2009 fogades till lagen en särskild bestämmelse om användning av fingeravtrycksuppgifter i pass för andra ändamål än de som uppgifterna har samlats in och registrerats för (lagens 16 a §). Fingeravtrycksuppgifter får användas för andra ändamål än de som uppgifterna har samlats in och registrerats för endast om det är nödvändigt för att identifiera ett offer för en naturkatastrof, storolycka eller någon annan katastrof eller för ett brott eller ett offer som annars förblivit oidentifierat. Genom den lagändring som trädde i kraft år 2014 utvidgades 16 a § till att gälla även fingeravtrycksuppgifter som hör till uppgifterna för identifiering av utlänningar. Bestämmelser om det ursprungliga ändamålet för insamling och registrering av uppgifter för identifiering av utlänningar finns i 131 § i utlänningslagen (301/2004). Grundlagsutskottet har i sitt utlåtande (GrUU 47/2010 rd) förutsatt att användningen av fingeravtryck som tas med stöd av 131 § i utlänningslagen ska begränsas uteslutande till ändamål som svarar mot det ändamål som de samlats in och registrerats för.

Enligt utskottet kan ett sådant ändamål i sig också ha samband med att hindra och utreda exakt angivna brott, men bara i den omfattningen som verksamheten har ett samband med det ursprungliga insamlings- och registreringsändamålet.

I kapitlets 17 § föreskrivs om utlämnande av uppgifter ur ett enhetsspecifikt personregister till en annan polisenhet för det ändamål som uppgifterna har samlats in och registrerats för och i 18 § föreskrivs om utlämnande av uppgifter till en annan polisenhet för andra ändamål än de som uppgifterna har samlats in och registrerats för. Kapitlets 19 § innehåller bestämmelser om utlämnande av uppgifter till andra myndigheter. Liksom 13 §, som gäller rätten att få uppgifter, bygger också 19 § dels på hänvisningar till andra lagar, dels på föreskrifter om de ändamål som uppgifter kan utlämnas för. Paragrafen i fråga har ändrats flera gånger och har därför blivit relativt svårtolkad. I avsnittet om bedömning av nuläget bedöms bestämmelserna om utlämnande av uppgifter parallellt med bedömningen av lagens 13 §, som gäller polisens rätt att få uppgifter från andra myndigheter.

5 kap.

I 22–26 § föreskrivs, separat för varje informationssystem, om utplåning och arkivering av uppgifter ur polisens personregister. Bestämmelserna om utplåning motsvarar till sin systematik bestämmelserna om registrering av uppgifter. Av bestämmelserna om utplåning kan nämnas den korta förvaringstiden på 6 månader som gäller för observationsuppgifter i informationssystemet för polisärenden och den bestämmelse om utplåning som gäller det nuvarande informationssystemet för misstänkta. Enligt 24 § ska uppgifter ur informationssystemet för misstänkta utplånas då tio år har förflutit sedan den sista uppgiften om ett misstänkt brott infördes.

I 27 § föreskrivs om uppgifter som konstaterats vara felaktiga. Trots bestämmelserna i personuppgiftslagen får en uppgift som konstaterats vara felaktig bevaras tillsammans med den korrigerade uppgiften, om det behövs för att trygga de rättigheter som den registrerade, någon annan part eller en person som hör till polispersonalen har. En sådan uppgift får användas endast i detta syfte. Lagens 28 § innehåller bestämmelser om arkivering av uppgifter och hänvisningar till arkivlagen (831/1994).

6 kap.

Lagens 6 kap. innehåller specialbestämmelser om behandling av uppgifter i samband med internationellt polissamarbete. Enligt 29 § får uppgifter lämnas ut till en medlemsstat i Europeiska unionen och under vissa i 30 § angivna förutsättningar även till stater utanför Europeiska unionen. I 31 § föreskrivs om behandling av uppgifter som fåtts från en annan stat eller ett internationellt organ. Särskilda bestämmelser om Schengens informationssystem finns i 32–37 §. Dessutom innehåller kapitlet hänvisningsbestämmelser till lagen om genomförande av vissa bestämmelser i beslutet om Europol (38 §), Eurodacförordningen (39 §), behandling av uppgifter som grundar sig på Prümfördraget och Prümrådsbeslutet (40 §), lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009) (41 §) samt Europaparlamentets och rådets förordning om Europeiska unionens informationssystem för viseringar (42 §).

7 kap.

Lagens 7 kap. innehåller bestämmelser om den registrerades rättigheter. I 43 § föreskrivs om polisens allmänna skyldighet att informera om behandling av uppgifter. Polisens skyldighet att

fullgöra sin informationsskyldighet enligt 24 § 1 mom. i personuppgiftslagen har i 43 § begränsats till att gälla situationer där personuppgifter samlats in för skötseln av de uppgifter som avses i 1 kap. 1 § 2 mom. i polislagen. Motsvarande informationsskyldighet gäller inte vid behandling av uppgifter som behövs för skötseln av uppgifter som avses i 1 kap. 1 § 1 mom. i polislagen.

I 44 och 47 § föreskrivs om den registrerades rätt till insyn. Enligt 44 § tillämpas i fråga om utövande av rätten till insyn 26 och 28 § i personuppgiftslagen. Med avvikelse från kraven i personuppgiftslagen ska en registrerad som vill utöva sin rätt till insyn dock på förhand framställa en personlig begäran om detta till den registeransvarige eller någon annan av denna utsedd polisenhet samt styrka sin identitet. En begäran om kontroll som gäller Schengens informationssystem kan enligt 47 § framställas antingen till en polisinrättning eller till dataombudsmannen.

Bestämmelser om inskränkningar av rätten till insyn finns i 45 §. På inskränkningarna i rätten till insyn tillämpas de inskränkningsgrunder som fastställs i 27 § personuppgiftslagen. Paragrafens 1 mom. innehåller dessutom en förteckning över de register och typer av information som den registrerades rätt till direkt insyn inte gäller. På dessa uppgifter tillämpas emellertid en indirekt rätt till insyn; dataombudsmannen kan på begäran av den registrerade kontrollera att uppgifterna är lagenliga.

Polisstyrelsen har den 23 januari 2012 utfärdat en anvisning om hur den registrerades rättigheter ska tillgodoses hos polisen (Tillgodoseendet av den registrerades rättigheter hos polisen: rätt till insyn, rättelse av uppgift och information 2020/2012/66). Enligt denna anvisning kan den registrerade framställa en begäran om tillgodoseende av sina rättigheter antingen hos den personuppgiftsansvarige eller hos vilken polisinrättning som helst.

8 kap.

Lagens 8 kap. innehåller särskilda bestämmelser. I 47 a § föreskrivs om skyddsåtgärder i civilrättsliga frågor. I 48 § föreskrivs om utfärdande av närmare bestämmelser och anvisningar. Lagens 49 § är en ikraftträdandebestämmelse.

2.2 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

EU-lagstiftningen om dataskydd

De två huvudsakliga målen med 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 (personuppgiftsdirektivet) har varit att säkerställa skyddet för personuppgifter som en grundläggande rättighet och det fria flödet av personuppgifter på den inre marknaden. Personuppgiftsdirektivet tillämpas på behandling av personuppgifter som utförs av såväl myndigheter som företag. Direktivet har kompletterats med flera specifika rättsakter, inklusive det s.k. direktivet om integritet och elektronisk kommunikation, datalagringsdirektivet och rådets rambeslut 2008/977/RIF, som tillämpas på polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet). Dataskyddsrambeslutet tillämpas på behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete, som bygger på avdelning VI i fördraget om Europeiska unionen. Dataskyddsrambeslutets tillämpningsområde omfattar således inte behandling av personuppgifter på nationell nivå, utan enbart utlämnande av personuppgifter mellan EU-medlemsstaternas behöriga myndigheter. Rambeslutet innehåller också en artikel om dels överföring av personuppgifter till tredjeländer och internationella organisationer, dels utlämnande av personuppgifter till privata aktörer som

är belägna i medlemsstater, och i dess 26 artikel föreskrivs om rambeslutets förhållande till avtal som ingåtts med tredjeländer.

Personuppgiftsdirektivet och dataskyddsrambeslutet ersätts med en ny EU-lagstiftning om dataskydd. Europeiska kommissionen lade den 29 januari 2012 fram ett förslag till dataskyddsdirektiv KOM (2012) 10 slutlig och ett förslag till dataskyddsförordning KOM (2012) 11 slutlig. Reformförslaget innefattar ett förslag till direktiv som ska stärka de bestämmelser som skyddar personuppgifter i sådana situationer där dessa uppgifter behandlas för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (dataskyddsdirektiv) och ett förslag till förordning som är avsett att stärka EU:s allmänna dataskyddsram (dataskyddsförordning). Dessa akter utfärdades den 27 april 2016. Den nya EU-lagstiftningen om dataskydd grundar sig på artikel 16.2 i fördraget om Europeiska unionens funktionssätt, som är den nya rättsliga grund för lagstiftning om personuppgiftsbehandling som införts genom Lissabonfördraget. Enligt den kan unionen utfärda lagstiftning om behandling av personuppgifter inom de områden som omfattas av unionsrättens tillämpningsområde. Målet med lagstiftningsreformen är att bygga ett modernt, starkt, enhetligt och heltäckande dataskyddsram för Europeiska unionen, stärka individens rättigheter och uppgiftsskyddet med avseende på den inre marknaden, justera de dataskyddsbestämmelser som gäller polissamarbete och straffrättsligt samarbete, beakta dataskyddets globala räckvidd i synnerhet när det gäller digitala tjänster samt effektivisera tillsynen över genomförandet av dataskyddsbestämmelserna.

Rätten till personuppgiftsskydd är en grundläggande rättighet som fastställs i artikel 16.1 i fördraget om Europeiska unionens funktionssätt och i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Artikeln har också nära samband med artikel 7 i stadgan om de grundläggande rättigheterna, som garanterar skyddet för privatlivet, och artikel 8 i Europakonventionen. Enligt EU-domstolens rättspraxis är rätten till personuppgiftsskydd dock inte ovillkorlig, utan den måste betraktas i ljuset av sin samhällsfunktion. Rätten kan begränsas, förutsatt att begränsningarna står i rätt proportion till det uppsatta målet. Personuppgiftsskyddet har också beröringspunkter med de övriga grundläggande rättigheterna som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna.

Dataskyddsförordningen har allmän räckvidd och är direkt tillämplig rätt som inte kräver något särskilt genomförande med undantag av kompletterande bestämmelser. Den kompletterande lagstiftning som behövs innefattar exempelvis bestämmelser om dataskyddsmyndigheter, rättsskydd och påföljder samt bestämmelser om rättsgrunderna för uppgiftsbehandlingen i vissa situationer som förordningen möjliggör. Nationell kompletterande lagstiftning är dessutom nödvändig exempelvis i situationer där behandlingen av personuppgifter grundar sig på den personuppgiftsansvariges lagstadgade skyldighet eller där behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller för den personuppgiftsansvariges myndighetsutövning.

Förordningens och direktivets bestämmelser om de allmänna principerna för behandlingen av personuppgifter, den personuppgiftsansvarige och behandlingen av personuppgifter samt dataskyddsmyndigheterna motsvarar huvudsakligen varandra. Syftet med detta är att säkerställa att de allmänna kraven på behandlingen av personuppgifter är så enhetliga som möjligt oberoende av medlemsstat eller personuppgiftsansvarig. De väsentligaste skillnaderna mellan rättsakterna ligger i att den behandling av personuppgifter som utförs av myndigheter inom direktivets tillämpningsområde har den särskilda karaktären av brottmål, i synnerhet till den del det är fråga om möjligheterna att inskränka den registrerades rättigheter i sådana fall som hör till direktivets tillämpningsområde. Förordningens tillämpningsområde omfattar i regel all behandling av personuppgifter som utförs av myndigheter, om behandlingen inte hör till direktivets tillämpningsområde.

Europarådets konventioner

Med stöd av dataskyddsförordningen och dataskyddsdirektivet kan Europeiska kommissionen fatta beslut om vilken nivå som är tillräcklig när det gäller tredjeländers dataskydd, och dessa beslut är av betydelse vid överföringen av personuppgifter till tredjeländer. När kommissionen fattar dessa beslut ska den bedöma vilka internationella skyldigheter landet i fråga har, framför allt avtalsförpliktelserna när det gäller dataskydd. Inom ramen för Europarådet antogs år 1981 en konvention (nr 108) om skydd för personuppgifter, som det hänvisas till i skäl 68 i dataskyddsdirektivet. Europarådets konvention och lagen om godkännande av vissa bestämmelser i den (269/1992) har i Finland satts i kraft genom en förordning (36/1992). I situationer mellan medlemsstaterna i Europeiska unionen tillämpas i första hand EU:s dataskyddslagstiftning, men alla EU-medlemsstater har ratificerat konvention nr 108. Sammanlagt 50 stater har tills vidare ratificerat konventionen. Det finns ett tilläggsprotokoll (nr 181) till konventionen som gäller gränsöverskridande uppgiftsflöden.

Bestämmelserna i konventionen erbjuder ett minimiskydd vid behandlingen av personuppgifter för alla personer som vistas i de stater som ratificerat den samt vid gränsöverskridande överföringar av personuppgifter. När det gäller överföring av personuppgifter tillämpas Europarådets konvention utöver de bestämmelser i förordningen och direktivet som gäller tredjeländer exempelvis i sådana situationer där en behörig myndighet i en EU-medlemsstat överför personuppgifter till ett tredjeland. Det är emellertid också möjligt att ett bilateralt avtal som ingåtts med landet i fråga kan bli tillämpligt, om det innehåller bestämmelser om dataskydd eller bestämmelser som hänvisar till den nationella lagstiftningen. Europarådets konvention omarbetas för tillfället, och den nya konventionen ersätter konvention nr 108 när tillräckligt många av Europarådets medlemsstater har ratificerat den. Det är möjligt att begränsa tillämpningen av bestämmelserna i konventionen om allmänintresset väger tyngre, t.ex. på grundval av den nationella säkerheten och det nationella försvaret.

Europarådet har även vissa andra konventioner som innehåller bestämmelser om behandlingen av personuppgifter. Ur polisverksamhetens perspektiv är i synnerhet konvention nr 185, som gäller bekämpning av it-relaterad brottslighet, och dess tilläggsprotokoll nr 189 av betydelse. Konventionen om it-brottslighet tillämpas bl.a. på frysning av personuppgifter inför ett rättshjälpsförfarande.

Vidare har Europarådet utfärdat en rekommendation R(87)15 om behandling av personuppgifter inom polissektorn. Europarådet har senast år 2013 låtit utreda hur rekommendationen har genomförts i Europarådets medlemsstater. Utredningen visar att rekommendationen som helhet har genomförts på rätt bred front, och det bedöms inte finnas något behov av brådskande tilläggsåtgärder i fråga om polissektorn. I utredningen noteras dock att lagstiftningen i Europarådets medlemsstater inte till alla delar är på den nivå som förutsätts för EU:s del i Europeiska kommissionens direktivförslag. Det rekommenderas i utredningen att man bör överväga att införa ett rättsligt bindande instrument för behandlingen av personuppgifter vid brottsbekämpningsmyndigheterna, och samtidigt ge akt också på underrättelsemyndigheternas verksamhet och den nationella säkerheten. Enligt utredningen kunde man välja mellan att anta en täckande konvention, vars tillämpningsområde även omfattar behandlingen av personuppgifter hos polisen, eller att foga ett separat tilläggsprotokoll antingen till konventionen om dataskydd eller till konventionen om it-brottslighet.

Bestämmelserna om passageraruppgifter

Passageraruppgifter och analysen av dessa spelar en allt viktigare roll i bekämpningen av brottslighet. I synnerhet insikten om att uppgifterna om flygpassagerare är nyttiga vid brottsbekämpningen har resulterat i att ett ökande antal stater eftersträvar att effektivisera möjlig-

heterna att utnyttja dessa uppgifter även internationellt genom att ålägga lufttrafikföretag skyldigheter att överlämna passageraruppgifter inom flygtrafiken (passenger name record, nedan PNR-uppgifter) till brottsbekämpningsmyndigheten i det egna landet.

Vissa länder utanför EU har under de senaste åren framställt krav på EU:s medlemsstater om överföring av PNR-uppgifter som gäller flygpassagerare. EU har förhandlat och förhandlar för närvarande om avtal om överlämnande av uppgifter i syfte att åstadkomma en rättslig grund och en tillräcklig nivå på dataskyddet för de uppgifter som ska överlämnas. För tillfället har EU gällande bilaterala avtal om överlämnande av PNR-uppgifter med Australien (VL L 186/14 14.7.2012) och Amerikas förenta stater (VL L 215/5 11.8.2012). Avtalen trädde i kraft sommaren 2012. Förhandlingar om överlämnande av uppgifter pågår för tillfället med Kanada (U 67/2013 rd).

Statsrådet har i juni 2013 lämnat en utredning om Rysslands påbud om överlämnande av passageraruppgifter inom flygtrafiken (E 87/2013 rd). Även många andra länder utanför EU, t.ex. Sydkorea, Japan, Qatar, Mexiko, Brasilien och Förenade Arabemiraten, har enligt kommissionen framställt eller ämnar framställa krav på EU:s medlemsstater om överlämnande av PNR-uppgifter om flygpassagerare.

Europeiska kommissionen offentliggjorde år 2007 ett förslag till rådets rambeslut om användande av passageraruppgifter i brottsbekämpningssyfte (U 3/2008 rd). Syftet med förslaget var att EU:s egna brottsbekämpande myndigheter skulle få använda PNR-uppgifter inom flygtrafiken vid bekämpningen av terrorism och grov brottslighet. Förslaget hann emellertid inte antas innan Lissabonfördraget trädde i kraft, och därför förföll förslaget vid övergången till den nya rättsgrunden. Av denna anledning offentliggjorde kommissionen ett direktivförslag i februari 2011 (U66/2010 rd), och Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet utfärdades den 27 april 2016. Medlemsstaterna ska sätta i kraft de bestämmelser som är nödvändiga för att följa direktivet senast den 25 maj 2018.

[Kompletteras i samband med den fortsatta beredningen.]

Annan EU-lagstiftning som innehåller bestämmelser om behandlingen av personuppgifter

Bestämmelser om behandlingen av personuppgifter hos polisen finns också i vissa EU-rättsakter med tillhörande genomförandelagar som tillämpas på sådant polissamarbete mellan EU-medlemsstater som anknyter till de uppgifter som avses i bestämmelsen om tillämpningsområde i dataskyddsdirektivet. Bland dessa rättsakter kan särskilt nämnas Europaparlamentets och rådets förordning (EG) nr 1987/2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II), rådets beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) samt Europaparlamentets och rådets förordning (EG) nr 1986/2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon; (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europolförordningen; och lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning, 214/2017); Europaparlamentets och rådets förordning (EU) nr 603/2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål (Eurodacförordningen); rådets beslut 2008/615/RIF om

ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet samt beslutet om dess genomförande 2008/616/RIF; samt rådets rambeslut 2006/960/RIF om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (och lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan brottsbekämpningsmyndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009).

Utländsk lagstiftning

Den nya EU-lagstiftningen om dataskydd har i fråga om polisens verksamhet tills vidare genomförts endast i Tyskland [och Danmark]. I Sverige har ett betänkande färdigställts om saken, inklusive en bilaga med förslag till genomförandelagstiftning. Betänkandet innehåller även observationer om den gällande lagstiftningen om behandling av personuppgifter i polisens verksamhet, inklusive resonemang om hur regleringen ska genomföras i fråga om Säkerhetspolisen i Sverige. I och med att syftet med propositionen är att genomföra EU-lagstiftningen om dataskydd och PNR-direktivet till den del dessa kompletterar den allmänna lagstiftningen om behandlingen av personuppgifter har det inte ansetts vara ändamålsenligt att göra någon omfattande internationell jämförelse av hur EU-lagstiftningen om dataskydd och PNR-direktivet genomförs, med tanke på att genomförandet är en pågående process i EU-medlemsstaterna. En jämförelse har emellertid gjorts i förhållande till vissa EU-medlemsstater som antingen har genomfört lagstiftningen eller låtit göra en omfattande utredning i frågan. Den gällande lagstiftningen i dessa stater har granskats som stöd för de övriga aspekterna för att bedöma om man i propositionen ska föreslå en registerbaserad regleringslösning eller en lösning som utgår från behandlingsändamålen när det gäller lagstiftningen om behandlingen av personuppgifter.

Sverige

Sverige har i sitt betänkande om genomförandet av dataskyddsdirektivet (SOU 2017:74, Brottsdatalag - kompletterande lagstiftning, Slutbetänkande av Utredningen om 2016 års dataskyddsdirektiv) föreslagit ett motsvarande tillämpningsområde för genomförandelagen som Finland, och lagen föreslås innehålla ett motsvarande begrepp för upprätthållande av den allmänna ordningen och säkerheten som den finska polislagen. I lagförslaget skiljer man mellan personuppgiftsbehandling som hänför sig till förebyggande av brottslighet, brottsbekämpning, verkställighet av straff eller allmän ordning och säkerhet. Vidare gör man skillnad mellan sådan personuppgiftsbehandling som omfattas av tillämpningsområdet för det lagförslag som gäller brottmål och sådan uppgiftsbehandling som hör till tillämpningsområdet för den allmänna dataskyddsförordningen. Lagförslagets innehåll motsvarar till stor del innehållet i dataskyddsdirektivet. I lagförslaget föreskrivs om sådan behandling av personuppgifter som är tillåten för de ändamål som anges i förslaget. Därtill föreslås i likhet med den gällande lagstiftningen en separat personregistersreglering för de enskilda myndigheter som hör till lagförslagets tillämpningsområde. De separata författningarna ska dock vara mindre detaljerade än de gällande lagarna, eftersom en stor del av deras bestämmelser ersätts av den nya brottsdatalagen. Den föreslagna lagen ska tillämpas av flera myndigheter, men endast till den del deras behandling av personuppgifter motsvarar de ändamål som hör till lagförslagets tillämpningsområde.

När det gäller Säkerhetspolisen är Sverige tvungen att på samma sätt som Finland tillämpa en nationell lösning, med tanke på att behandling av personuppgifter som hänför sig till ländernas nationella säkerhet inte hör till EU-rättens tillämpningsområde, men säkerhetspolisens behandling av personuppgifter omfattas av tillämpningsområdet för den gällande personuppgiftslagen för polisväsendet. I betänkandet föreslås att en separat nationell lag ska stiftas om be-

handlingen av personuppgifter vid säkerhetspolisen (förslag till Säkerhetspolisens datalag). Det lagförslag som gäller brottmål innehåller emellertid bestämmelser om behandlingen av personuppgifter vid säkerhetspolisen till den del behandlingen inte hänför sig till nationell säkerhet. Lagförslagets 9 kap. innehåller detaljerade bestämmelser om bl.a. ändamålen med behandlingen av personuppgifter, som preciserar den uppgiftsbehandling som hänför sig till nationell säkerhet, förvaringstiderna för personuppgifter, den registrerades rättigheter, dataskyddsmyndigheten och utlämnandet av personuppgifter. Beträffande säkerhetspolisen föreslås det dessutom att en kompletterande förordning med mer detaljerade bestämmelser om bl.a. säkerhetspolisens personregister ska utfärdas.

Sverige har med avseende på den gällande lagstiftningen omfattat samma typ av regleringslösning som Finland, i och med att behandlingen av personuppgifter vid polisen (Polismyndigheten) regleras genom en separat lag (polisdatalagen, 2010:361), som gäller behandling av personuppgifter i brottmål samt den personuppgiftsbehandling som utförs av Säkerhetspolisen. Lagen gäller automatiserad behandling av personuppgifter eller sådan behandling som sker i registerform. På övrig behandling av personuppgifter tillämpar polisen den allmänna personuppgiftslagen, såvida inte särskilda bestämmelser ska tillämpas, t.ex. i utlänningsärenden. I Sverige innefattar polisens behandling av personuppgifter även sådan behandling av personuppgifter som hänför sig till penningtvätt. Lagen innehåller hänvisningar till de bestämmelser i personuppgiftslagen som ska tillämpas också på sådan personuppgiftsbehandling som hänför sig till polisens brottsbekämpning, såsom de allmänna grunderna för uppgiftsbehandlingen, definitionerna, den registrerades rättigheter och kontroll samt skadestånd.

I polisdatalagen föreskrivs om de ändamål för vilka personuppgifter får behandlas (2 kap.). Förteckningarna är uttömmande, men bestämmelserna är tämligen allmänna. Dessa behandlingsändamål har delats in i primära och sekundära ändamål. De primära ändamålen hänför sig till sådana personuppgifter som behövs för att förebygga, avslöja eller utreda brott eller för att fullgöra internationella skyldigheter. De sekundära ändamålen hänför sig till utlämnande av personuppgifter till andra myndigheter antingen för deras egna behov eller för annan polisiär verksamhet. Personuppgifter får lämnas ut för sekundära behandlingsändamål när den mottagande myndigheten behöver uppgifterna för brottsbekämpning. Exempel på sådana myndigheter är Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, samt behöriga utländska myndigheter och internationella organisationer. Personuppgifter kan överlåtas till polisen också för andra behandlingsändamål än det ursprungliga ändamålet, när det nya ändamålet är förenligt med det ursprungliga.

Personuppgifter får också behandlas om det är nödvändigt för diarieföring, för handläggning av en anmälan som gjorts till polisen eller i övrigt för behandlingen av ett ärende. I lagen föreskrivs också om situationer där personuppgifter trots bestämmelserna om sekretess får överlåtas bl.a. till Interpol och Europol, en utländsk underrättelsemyndighet eller någon annan utländsk myndighet eller en internationell organisation, samt till ovan nämnda svenska myndigheter.

I polisdatalagen föreskrivs dessutom om behandlingen av känsliga personuppgifter, behandlingen av personuppgifter vid ett kriminaltekniskt laboratorium samt vissa register (4 kap.), närmare bestämt DNA-registret, utredningsregistret, spårregistret, fingeravtrycksregistret, signalementsregistret, penningtvättsregistret och det internationella registret. Bestämmelserna om registren är tämligen enkla, och även i fråga om dessa register föreskrivs det om ändamålet med behandlingen av personuppgifter. Regleringen av registren kompletteras emellertid av polisdataförordningen (2010:1155), där det preciseras vilka personuppgifter som får införas i polisens register och vilka personuppgifter som får göras tillgängliga för andra myndigheter genom sökning.

Den gällande svenska polisdatalagen är en kombination av behandlingsändamålsbaserade och registerbaserade bestämmelser, men huvudvikten ligger på bestämmelser som utgår från behandlingsändamålen. Lagen innehåller också bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet (6 kap.) I samma kapitel föreskrivs om behandlingsändamålen, som delvis avviker från ändamålen med behandlingen av personuppgifter i polisens verksamhet, samt om bevarande och gallring. I fråga om utlämnande av personuppgifter gäller huvudsakligen samma bestämmelser som för polisen. Polisdatalagen innehåller dessutom bestämmelser om lagens förhållande till den EU-lagstiftning som ska tillämpas på polissamarbete, vilken innehåller bestämmelser om behandling av personuppgifter.

I betänkandet om genomförandet av dataskyddsdirektivet föreslås det att polisdatalagen och den tillhörande förordningen ska ges nya namn (förslag till lag om ändring i polisdatalagen, förslag till förordning om ändring i polisdataförordningen - polisens brottsdatalag, polisens brottsdataförordning). Det föreslås också att bestämmelserna om polisens personregister ska koncentreras avsevärt och deras innehåll anpassas till det nya regelverket. Lagen ska alltjämt innehålla bestämmelser om behandlingsändamålen. De ska emellertid överensstämma med de behandlingsändamål för personuppgifter som anges i dataskyddsdirektivet. Därtill ska lagen i likhet med den gällande lagen innehålla bestämmelser om vissa personregister och om utlämnande av personuppgifter. Enligt förslaget ska innehållet i bestämmelserna om registren till vissa delar preciseras. Lagen ska dessutom i detalj fastställa vilka myndigheter som medges direktåtkomst till registren och vilka personuppgifter som i övrigt kan lämnas ut. På motsvarande sätt som den gällande regleringen ska lagförslaget kompletteras av en förordning, som till sitt innehåll huvudsakligen motsvarar den gällande polisdataförordningen.

I Sverige har ett separat betänkande beretts med avseende på genomförandet av PNR-direktivet (Betänkande av PNR-utredningen, SOU 2017:57). Betänkandet innehåller ett förslag till en ny lag om flygpassageraruppgifter i brottsbekämpningen.

Tyskland

Tyskland har redan genomfört det nya dataskyddsdirektivet och PNR-direktivet på förbundsstatsnivå. Bestämmelserna om genomförandet av PNR-direktivet finns i en separat lag. Bestämmelserna om genomförande av dataskyddsdirektivet finns i 45–84 § i förbundsstatens dataskyddslag (BDSG) och i avdelning 1 i lagen, som gäller alla behandlingsändamål för personuppgifter. Bestämmelserna tillämpas i enlighet med bestämmelsen om tillämpningsområde i direktivet på sådan behandling av personuppgifter som utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten. Bestämmelserna gäller tyska myndigheter till den del dessa sköter ovannämnda uppgifter. Som brott betraktas sådana handlingar som enligt den tyska strafflagen definieras som brott.

De allmänt tillämpliga bestämmelserna kompletteras i Tyskland av såväl bestämmelserna i förbundsstatens lag om kriminalpolisen som lagstiftningen om de regionala polismyndigheterna. Lagen om kriminalpolisen på förbundsstatsnivå (Bundeskriminalamt, BKA) innehåller vissa bestämmelser som preciserar dataskyddslagens bestämmelser med avseende på BKA:s behandlingsändamål. Som exempel kan nämnas framför allt bestämmelserna om inhämtning av uppgifter i avdelning 2 samt bestämmelserna om internationellt utlämnande av personuppgifter (25–28 §), där det föreskrivs separat om utlämnande av uppgifter inom landet, utlämnande av uppgifter till EU-medlemsstater och internationellt utlämnande av uppgifter. Ytterligare bestämmelser om behandling av personuppgifter finns särskilt i avdelning 9, där det bl.a. fastställs för vilka ändamål BKA får behandla personuppgifter.

Lagen om polisverksamheten på förbundsstatsnivå innehåller detaljerade bestämmelser om inhämtning av uppgifter och om de vidarebehandlingsändamål för vilka de inhämtade uppgifterna får behandlas. I lagen föreskrivs om förbundsstatens polisdatasystem (13 §), vars datainnehåll grundar sig på polisens uppgifter på förbundsstatsnivå. Bestämmelsen är tämligen allmänt formulerad men anknyter till övrig EU-lagstiftning och nationell lagstiftning som gäller polisens uppgifter samt till bestämmelserna om informationsinhämtning. Regleringen av polisen på förbundsstatsnivå utgör således en kombination av datasystemsspecifik och behandlingsändamålsbaserad reglering. I övrigt finns det inga detaljerade bestämmelser om behandlingsändamål, med undantag av vissa vidarebehandlingsändamål för personuppgifter, såsom forskning. I lagen föreskrivs i detalj om behandlingen av DNA-uppgifter, men inte om behandlingen av andra känsliga personuppgifter. De krav som ställs på behandlingen av andra känsliga personuppgifter grundar sig direkt på dataskyddslagen. Lagen innehåller en detaljerad förteckning över de kategorier av personer vars personuppgifter (såsom grundläggande personuppgifter) polisen får behandla.

Den tyska lagstiftningen om behandling av personuppgifter är när det gäller polisen indelad i förbundsstatslagstiftning och regional (Länder) lagstiftning. Det ovan nämnda polisdatasystemet på förbundsstatsnivå är ett system som administreras enbart av BKA. Det är emellertid anslutet till en större datanätshelhet (29 §), som används även av de regionala polismyndigheterna i enlighet med vad som föreskrivs i den regionala polislagstiftningen. Alla personuppgifter som behandlas av BKA eller de regionala polismyndigheterna lagras dock inte i det riksomfattande datanätet.

2.3 Bedömning av nuläget

Lagens struktur

Enligt förslaget ska lagens struktur och innehåll omarbetas i sin helhet. Liksom det har konstaterats i grundlagsutskottets utlåtande GrUU 18/2012 rd och förvaltningsutskottets betänkande FvUB 26/2013 rd har lagen blivit komplicerad till såväl struktur som innehåll. Lagen innehåller dessutom flera överlappningar med de allmänna lagarna om behandling av personuppgifter. Den gällande lagen har vissa drag av överreglering även i det avseendet att den innehåller bestämmelser om polisens rättigheter att få och lämna ut uppgifter trots att det redan finns bestämmelser om detta i andra lagar. Det föreskrivs om utlämnande av uppgifter och rätt att få uppgifter såväl i den lagstiftning som gäller den utlämnande myndigheten och i lagstiftningen om den mottagande myndigheten. Detta regleringssätt är problematiskt för den som ska tillämpa lagen, eftersom informationsutbytets lagenlighet måste kontrolleras i minst två olika speciallagar som gäller en myndighet. Lagtekniskt sett har denna typ av dubbel reglering dock blivit vanlig i det finländska rättssystemet.

Den gällande personuppgiftslagen för polisväsendet verkar innehålla inte bara onödiga eller överdrivet detaljerade bestämmelser utan också sådana bestämmelser som är mycket abstrakt formulerade. Detta är problematiskt framför allt med tanke på att regleringen gäller skyddet för personuppgifter. Som exempel kan nämnas de allmänna definitionerna av ändamålet med personuppgifterna samt undantagsbestämmelserna om dessa. Det föreslås att bestämmelserna om behandlingen av uppgifter ska vara mer exakta, så att principen om ändamålsbegränsning uppfylls konsekvent med avseende på polisens olika informationssystem.

Det faktum att personuppgiftslagen för polisväsendet är så detaljerad gör att lagen behöver ändras ofta. Lagens struktur behöver förtydligas lagtekniskt sett. Samtidigt föreslås det att bestämmelser som överlappar med och är onödiga i förhållande till den allmänna lagstiftningen om personuppgiftsbehandling stryks och att lagens detaljerade karaktär, som ger upphov till kontinuerliga ändringsbehov, frångås.

Tillämpningsområde och lagens syfte

Bestämmelser om polisens uppgifter finns i 1 kap. 1 § i polislagen. Bestämmelser om polisens befogenheter att inhämta information som behövs för att förebygga och avslöja brott finns i polislagen, och bestämmelser om befogenheterna att inhämta information som behövs för brottsutredning finns i tvångsmedelslagen och förundersökningslagen. I det 1:a lagförslaget i propositionen föreskrivs om sådan behandling av personuppgifter som grundar sig på de uppgifter och befogenheter som anges i dessa gällande bestämmelser. Det 1:a lagförslaget i propositionen innehåller inga bestämmelser om befogenheter, utan enligt förslaget ska det i lagen föreskrivas om de ändamål för vilka polisen får behandla personuppgifter för att kunna utföra sina uppgifter. Polisens grundläggande uppgifter och ändamål med behandlingen av personuppgifter har inte förändrats efter att den gällande personuppgiftslagen för polisväsendet stiftades, och tillämpningsområdet för personuppgiftslagen för polisväsendet förändras inte heller.

Däremot har det skett många förändringar i polisens operativa miljö och i de strategiska tyngdpunkterna i polisens verksamhet. Som exempel kan nämnas att hotet om terrorism har ökat i hela Europa, och dessutom är gränsöverskridande organiserad brottslighet och rörliga, mindre kriminella sammanslutningar ett växande fenomen. Även it-brottsligheten har ökat. Den betydande ökningen i antalet asylsökande som söker sig till Europa är en annan faktor som har gjort att polisens uppgifter ökat i antal. Ett fungerande informationsflöde är en central verksamhetsförutsättning för ett nätverksbaserat samhälle som strävar efter riskhantering. För att kunna reagera på förändringar i den säkerhetspolitiska omgivningen måste myndigheterna ha en bättre lägesmedvetenhet och framförhållning och bedriva tätare samarbete. Samhället blir allt känsligare för störningar och det är därför viktigt att myndigheterna kan reagera snabbt och effektivt på förändringar. För polisens del rör förändringarna i den säkerhetspolitiska omgivningen den allmänna ordningen och säkerheten samt, i relation till detta, brottslighet samt strävan efter att förebygga eller utreda brott eller föra brott till åtalsprövning. En rätt inriktad myndighetsverksamhet bygger på riktig information som fås i så nära realtid som möjligt. Det föreslås att bestämmelserna om utlämnande av personuppgifter i den gällande lagen ska förtydligas med beaktande av polisens behov av omfattande samarbete med andra myndigheter. I bestämmelserna om utlämnande av uppgifter ska det också tas hänsyn till de krav som ställs i EU-lagstiftningen om dataskydd. Vidare ska det i det 1:a lagförslagets bestämmelser om behandlingsändamål för personuppgifter ges akt på polisens behov av att under vissa förutsättningar jämföra uppgifter om en och samma person som införts i olika register, t.ex. för att bilda en hotbedömning. Om dessa förutsättningar föreskrivs i en bestämmelse om förenlig behandling av personuppgifter. Det föreslås att bestämmelsen i fråga ska justeras jämfört med den gällande lagen.

Riksdagens grundlagsutskott har vid bedömningen av den föregående totalreformen av lagen konstaterat i sitt utlåtande GrUU 51/2002 att lagen ska innehålla bestämmelser om syftet med registreringen. Grundlagsutskottet konstaterade att detta indirekt framgår av den i 1 § uttryckta anknytningen till skötseln av de uppgifter som avses i 1 kap. 1 § polislagen samt hänvisningarna till informationssystemet för polisärenden (2 §), informationssystemet för förvaltningsärenden (3 §) och informationssystemet för misstänkta (4 §) Grundlagsutskottet ansåg dock att en reglering av detta slag lätt blir generell och summarisk, vilket gör det möjligt för myndigheterna att själva i stor utsträckning bestämma innehållet i och omfattningen av de registrerade personuppgifterna. Utskottet konstaterade emellertid att någon risk för detta inte fanns i den föreliggande propositionen, eftersom bestämmelserna i 2 kap. i allmänhet tillräckligt noggrant anger vilka uppgifter som får registreras i informationssystemet.

Informationssystemet för polisärenden

Grundlagsutskottet och förvaltningsutskottet har inte ansett att innehållet i informationssystemet för polisärenden är problematiskt. Bestämmelsen om informationssystemet har emellertid till följd av flera ändringar blivit kanske t.o.m. något överdrivet detaljerad och svårläst, och dessutom skapar en del av de typer av information som räknas upp i paragrafen en viss oklarhet i förhållande till de övriga bestämmelserna i lagen. Exempelvis kategorin observationsuppgifter, som fogades till bestämmelsen år 2013, har orsakat en viss oklarhet i förhållande till de observationsuppgifter som avses i paragrafen om informationssystemet för misstänkta. Trots att bestämmelserna om informationssystemet för polisärenden uppfyller de i grundlagen angivna kraven på detaljerad och noggrant avgränsad reglering om behandling av personuppgifter föreslås det att bestämmelserna till denna del ska förenklas. Enligt förslaget ska dessutom behandling av personuppgifter för olika undersökningsändamål, såsom förundersökning och polisundersökning, och behandling av personuppgifter för upprätthållande av allmän ordning och säkerhet regleras i två olika bestämmelser.

Informationssystemet för förvaltningsärenden

Liksom i fråga om informationssystemet för polisärenden har problemet med informationssystemet för förvaltningsärenden ansetts vara att regleringen är för detaljerad när det gäller sådana uppgifter, utöver grundläggande personuppgifter, som behöver lagras i systemet för att ett ärende ska kunna behandlas. De detaljerade förteckningarna över olika typer av information i 3 § 3 mom., som gäller informationssystemet för förvaltningsärenden, har orsakat ett ofta återkommande behov av ändringar i lagen. Dessutom har regleringen av innehållet i de typer av information som gäller tillståndsärenden blivit oenhetlig till följd av alla ändringar som gjorts. Det föreslås att bestämmelsen ska förtydligas så att förteckningarna över olika typer av information stryks i den gällande lagen. Samtidigt ska det till den föreslagna 2 kap. 9 § fogas en förteckning som saknas i den gällande 3 §, nämligen en förteckning över de kategorier av registrerade vars uppgifter får behandlas för de ändamål som anges i paragrafen.

Enligt förslaget ska den gällande regleringen ändras också på så sätt att den föreslagna 2 kap. 9 § inte innehåller någon hänvisning till de uppgifter som fastställs i polislagens 1 kap. 1 §. Hänvisningen är problematisk i fråga om informationssystemet för förvaltningsärenden, eftersom 1 kap. 1 § 2 mom. i polislagen förutom tillståndsförvaltningsuppgifter även innehåller andra uppgifter som fastställs separat i lag för polisen, och behandlingen av personuppgifter för utförandet av dessa uppgifter i vissa fall hör till dataskyddsdirektivets tillämpningsområde. Det föreslås att ändamålet med personuppgifterna inte ska bindas till polislagen utan direkt till de lagar där det föreskrivs om polisens tillståndsförvaltningsuppgifter och tillsynsuppgifterna i anslutning till dessa. Till dessa lagar fogas som nya lagar även hittegodslagen (778/1988), lagen om skjutbanor (763/2015) samt lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017, lagen om penningtvätt). Den gällande 3 § innehåller inga bestämmelser om behandling av personuppgifter för utförande av de uppgifter som åläggs polisen i hittegodslagen och lagen om skjutbanor. I informationssystemet för förvaltningsärenden ska enligt den gällande lagen inte heller registreras information om de uppgifter för tillsyn över penningspelsverksamhet som åläggs polisen i lagen om penningtvätt och lotterilagen (1047/2001) och som hör nära samman med tillståndsförvaltning.

Informationssystemet för misstänkta

Förvaltningsutskottet har i sitt utlåtande (FvUU 40/2014 rd) fäst vikt vid vissa brister som förekommer i behandlingen av personuppgifter när det gäller informationssystemet för misstänkta. Personer kan registreras endast som misstänkta eller som misstänkta för medverkan till ett brott. Förvaltningsutskottet har i sitt betänkande (FvUB 16/2014 rd) konstaterat att när

uppgifter om en person förs in i registret över misstänkta måste kriterierna uppfyllas, det vill säga att personen kan misstänkas göra sig eller ha gjort sig skyldig alternativt medverka eller ha medverkat till ett brott. Tröskeln för "skäl att misstänka" är densamma som tröskeln för att inleda förundersökning av brott enligt förundersökningslagen (805/2011).

Att det inte är så enkelt att tillämpa bestämmelserna om registret över misstänkta framgår enligt förvaltningsutskottet av att registret inte bara innehåller uppgifter om misstänkta personer som har gjort sig skyldiga eller har medverkat till ett brott som nämns i bestämmelsen, utan också om ett sådant brott som personen kan göra sig skyldig eller medverka till i framtiden. Utskottet har ansett det vara uppenbart att misstanken i sådana fall måste grunda sig på konkreta iakttagelser som ger anledning att sluta sig till att personen kommer att handla så att kravet "skäl att misstänka" uppfylls på ett godtagbart sätt. Att bedöma hur en person kommer att bete sig i framtiden är kopplat till en så osäker slutledningskedja att risken för felbedömning är mycket stor.

Förvaltningsutskottet (FvUU 40/2014) har också fäst vikt vid att det i en kompletterande ”förklaringsdel” dessutom kan ha funnits anteckning om till exempel den mot vilken den misstänkte riktat eller kan rikta hot om våld. Detta har motiverats med att polisen i annat fall inte kan skydda denna person, som kan ses som målsägande. Till denna del har det alltså inte varit fråga om registrerade personer. Även grundlagsutskottet har redan tidigare fäst vikt vid att det i motiveringen anges att också uppgifter om potentiella eller verkliga brottsoffer får införas i informationssystemet för misstänkta såsom uppgifter som hänför sig till brottet. Lagförslagets 4 § omfattar dock inte detta syfte. (GrUU 51/2002 rd) Det att registrering av namn på brottsoffer nämns endast i motiveringen till bestämmelsen kan inte betraktas som sådan noggrant avgränsad reglering som förutsätts i grundlagsutskottets tolkningspraxis.

Bestämmelserna om informationssystemet för misstänkta har betraktats som oändamålsenliga och bristfälliga även med tanke på polisens verksamhet. Ordalydelsen i paragrafen verkar bygga på personbaserad kriminalunderrättelseinhämtning, dvs. att polisen måste känna till att en person är föremål för en konkret brottsmisstanke, och bestämmelserna omfattar inte i någon vidare bemärkelse exempelvis brottsanalys som riktas mot organiserad brottslighet eller kriminella sammanslutningar. Enligt motiveringen till bestämmelsen i regeringens proposition (RP 93/2002 rd) kan man dock på grund av syftet med registret över misstänkta inte förutsätta att individualiseringen av ett brott ska vara mycket precis. Detta gäller t.ex. den verksamhet som medlemmarna i en känd kriminell sammanslutning bedriver. Polisen har också upplevt det som problematiskt att bestämmelsen på grundval av ordalydelsen inte direkt har omfattat exempelvis registrering av faktiska eller potentiella brottsoffer, trots att detta konstateras i motiveringen till den ovannämnda regeringspropositionen.

Skyddspolisen

Inrikesministeriet har den 1 oktober 2015 tillsatt ett projekt i syfte att bereda förslag till en lagstiftning om civil underrättelseinhämtning. Enligt beslutet om tillsättande är det viktigaste målet med projektet att förbättra den nationella säkerheten. Ambitionen är att bereda de centrala bestämmelserna om civilunderrättelseinhämtning och på så sätt förbättra skyddspolisens informationsinhämtning i fråga om allvarliga internationella hot som sammanhänger med polisens uppgifter så att skyddspolisen har befogenheter till personbaserad underrättelseinhämtning som avser utländska förhållanden, underrättelseinhämtning som avser datasystem och underrättelseinhämtning som avser datatrafik. De bestämmelser som bereds inom ramen för projektet ska enligt beslutet om tillsättande samordnas med projektet för en lagstiftning om militär underrättelseinhämtning, som pågår samtidigt. Mandattiden för projektet för civil underrättelseinhämtning gick ut den 28 februari 2017.

Om skyddspolisen får nya befogenheter ska personuppgifter som hänför sig till information som inhämtats genom dessa nya befogenheter registreras i skyddspolisens funktionella informationssystem på samma sätt som sådana personuppgifter som hänför sig till information som inhämtats med hjälp av de redan befintliga befogenheterna. Med andra ord ska det föreskrivas om registrering och behandling av personuppgifter som inhämtats genom de nya befogenheterna i samma lag som det föreskrivs om registrering och behandling av andra personuppgifter vid skyddspolisen.

Vidare finns det skäl att beakta att det inom skyddspolisen pågår ett projekt vars främsta syfte är att utveckla och effektivisera skyddspolisens verksamhet, och ett av de mest centrala målen med projektet är att förnya skyddspolisens funktionella informationssystem. Mandattiden för projektet löper ut vid utgången av 2019.

Rätt att få uppgifter (i synnerhet 13 § i gällande lag)

Lagens 13 § innehåller bestämmelser om polisens rätt att få uppgifter ur vissa register och informationssystem. Paragrafen i fråga har ändrats flera gånger och har därför blivit relativt svårtolkad och detaljerad. Den innehåller hänvisningar till speciallagar, vilket ger upphov till ständiga lagändringsbehov. De många lagändringarna har också gjort regleringen oenhetlig ur olika mottagande parters perspektiv. Det har emellertid bedömts vara svårt att slopa bestämmelserna om rätten att få uppgifter bl.a. för att lagen i vilket fall som helst alltjämt måste innehålla den i 13 § 3 mom. angivna rätten för polisen att få de uppgifter som avses i paragrafen avgiftsfritt. Vidare föreskrivs det i 13 § 2 mom. om polisens rätt att få vissa uppgifter inom en skälig tid, och polisen kan också förena åläggandet med vite.

Utlämnande av uppgifter (i synnerhet 19 § i gällande lag)

Lagens 19 § innehåller bestämmelser om utlämnande av uppgifter till andra myndigheter. Även 19 § har ändrats flera gånger, och paragrafen har därför blivit relativt svårtolkad och detaljerad. Den innehåller paragrafspecifika hänvisningar till speciallagar, vilket ger upphov till återkommande lagändringsbehov allteftersom lagstiftningen om den mottagande parten ändras. Ändamålet med uppgifterna har dessutom definierats på olika sätt i fråga om olika mottagande parter.

Samtidigt omstrukturerades bestämmelserna om behandling av personuppgifter i internationellt polissamarbete i sin helhet år 2013 (RP 66/2012 rd). Bestämmelserna ändrades i enlighet med vad som förutsattes i internationella författningar. Till lagen fogades också nya bestämmelser om behandling av uppgifter som fås från utlandet. Lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet preciserades för att motsvara ändringarna i personuppgiftslagen för polisväsendet. I denna proposition föreslås inga betydande ändringar i dessa bestämmelser.

Intern laglighetskontroll

Polisstyrelsen granskar genom stickprov logguppgifterna minst två gånger per år för att kontrollera att registren används som sig bör. Vid Polisstyrelsen och de övriga polisenheterna granskas logguppgifterna också flera gånger per år för att utreda enskilda frågor som uppkommit.

Polisstyrelsen granskar alla operativa polisenheter årligen. De laglighetsgranskningar som gäller polisens hemliga informationsinhämtning och som i synnerhet fokuserar på systemet för

hemliga tvångsmedel utgör permanenta objekt för de årliga laglighetsgranskningarna. Dessutom granskas varje år de övriga registren som polisen använder i enlighet med Polisstyrelsens plan för laglighetsgranskningar. Polisenheten underrättas på förhand om en del av granskningarna, men inte om alla.

I samband med Polisstyrelsens årliga laglighetsgranskningar synas också polisenheternas egen laglighetskontroll. Polisenheternas laglighetskontroll grundar sig på en årlig plan, som även inkluderar en granskning av registren.

Extern laglighetskontroll

Förutom Polisstyrelsens och polisenheternas interna laglighetskontroll övervakar också dataombudsmannen lagenligheten vid behandlingen av personuppgifter för att uppfylla personuppgiftslagens syften. Dataombudsmannen har med stöd av personuppgiftslagen rätt att granska personregistren och anlita experter för granskningarna.

Utöver de regelmässiga granskningar som utförs av justitieombudsmannens byrå och statsrådets justitiekanslersämbete granskar även inrikesministeriet lagenligheten hos Polisstyrelsens verksamhet och behandling av personuppgifter. Polisförvaltningen samarbetar med dataskyddsmyndigheterna och laglighetskontrollmyndigheterna för att utveckla uppgiftsbehandlingen.

Även den registrerade kan kontrollera uppgifter om sig själv och kräva att uppgifter ska korrigeras inom de begränsningar som anges i lagen. Polisen informerar om den registrerades rättigheter för att göra det möjligt för honom eller henne att utnyttja sin rätt till insyn. De personuppgifter som polisen samlar in, ändamålet med uppgiftsbehandlingen, de sätt på vilka uppgifterna ska behandlas och skyddas samt den registrerades rättigheter beskrivs i registerspecifika dataskyddsbeskrivningar. När den registrerade vill utnyttja sin rätt till insyn ska han eller hon personligen framställa en begäran om detta hos polisen och styrka sin identitet. Dataombudsmannen får på begäran av den registrerade kontrollera att uppgifterna om den registrerade är lagenliga, när det är fråga om sådana uppgifter som den registrerades personliga rätt till insyn inte omfattar (s.k. indirekt rätt till insyn). Bestämmelser om utnyttjande av rätten till insyn ska också finnas i lagen om genomförande av dataskyddsdirektivet, som ska tillämpas som allmän lag på personuppgiftsbehandlingen inom polisväsendet, och i dataskyddslagen, som kompletterar dataskyddsförordningen.

Utveckling av tillsynen över registren

Förvaltningsutskottet har i sitt betänkande (FvUB 26/2013 rd) om regeringsproposition 66/2012 rd fäst vikt vid att den personuppgiftsansvarige enligt personuppgiftslagen (523/1999) bland annat ska se till att oriktiga, ofullständiga eller föråldrade personuppgifter inte behandlas. Dataombudsmannen har trots sekretessbestämmelserna rätt att få information om de personuppgifter som är föremål för behandling samt all den information som behövs för att övervaka att behandlingen av personuppgifter sker i enlighet med lag. Förvaltningsutskottet har bedömt om det för att säkerställa en effektiv övervakning borde föreskrivas exempelvis om en särskild skyldighet att årligen rapportera om behandlingen av observationsuppgifter till dataombudsmannen. Med beaktande av den korta lagringstid som gäller för observationsuppgifter, den registeransvariges skyldigheter enligt personuppgiftslagen, datasekretessmyndigheternas rätt att få information och utföra inspektioner samt med hänsyn till laglighetskontrollen i övrigt anser utskottet emellertid att tillsynen över behandlingen av observationsuppgifter kan ske på behörigt sätt utan någon särskild rapporteringsskyldighet.

Utskottet konstaterade dock allmänt taget i sitt betänkande att de nya typer av information som enligt propositionen ska få lagras och den närmare preciseringen av informationens innehåll utifrån behövlighetsprövning kräver extra satsningar på tillsynen över hur personuppgifter behandlas. Det är nödvändigt att övervaka behandlingen av personuppgifter med hänsyn till såväl uppgifternas innehåll som hur de används. Slutsatserna av övervakningen borde också rapporteras bättre. Det 1:a och 2:a lagförslaget i propositionen innebär att ännu fler nya typer av information ska få behandlas för att förebygga, utreda och avslöja brott, i synnerhet vissa personuppgifter med anknytning till kriminalunderrättelseinhämtning och passageraruppgifter. Behandlingsändamålen beskrivs i detalj i lagen, men i och med att den registerbaserade regleringen frångås förblir informationens innehåll tämligen oklart, förutom i fråga om de olika kategorierna av personer. Detta i kombination med att den personuppgiftsansvariges ansvar accentueras i den nya EU-lagstiftningen om dataskydd ställer särskilda krav på att de personuppgiftsansvariga fäster särskild vikt vid tillsynen över registren. EU:s allmänna dataskyddsförordning och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten innehåller detaljerade bestämmelser om den personuppgiftsansvariges skyldigheter, informationssäkerheten och övervakningen av personuppgiftsbehandlingen, inklusive skyldigheten att utnämna ett dataskyddsombud. Den nya regleringen anses i tillräcklig grad möta de utvecklingsbehov som riksdagen lyft fram.

3 Målsättning och de viktigaste förslagen

3.1 Målsättning

Det 1:a lagförslaget i propositionen kompletterar den allmänt tillämpliga lagstiftningen om genomförandet av dataskyddsdirektivet samt EU:s dataskyddsförordning och den kompletterande dataskyddslagen till den del de nödvändiga genomförandebestämmelserna inte ingår i de nämnda författningarna. Den viktigaste målsättningen med propositionen är att den nya personuppgiftslagen för polisväsendet uppfyller kraven i EU-lagstiftningen om dataskydd, med beaktande av brottsbekämpningsbehoven och kraven på skyddet för de grundläggande och mänskliga rättigheterna. Genom det 2:a lagförslaget i propositionen genomförs till behövliga delar bestämmelserna om personuppgiftsbehandling i PNR-direktivet.

Enligt artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt artikel 8.1 i stadgan har var och en rätt till skydd för de personuppgifter som rör honom eller henne. Enligt artikel 8.2 ska dessa uppgifter behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Europeiska domstolen för de mänskliga rättigheterna har i sin rättspraxis ansett att artikel 8 i Europakonventionen, som gäller skyddet för privatliv, ska tillämpas på registrering av personuppgifter som rör en persons privatliv. Domstolen har konstaterat att en överträdelse av konventionen har skett bl.a. i sådana fall där den nationella lagstiftningen inte har innehållit bestämmelser om vad uppgifterna får innehålla, hur länge de får förvaras och om vilka personkategorier uppgifter får samlas in.

Enligt 10 § 1 mom. i grundlagen utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Enligt grundlagsutskottets vedertagna praxis begränsas lagstiftarens spelrum förutom av denna bestämmelse även av att skyddet för personuppgifter delvis ingår i skyddet för privatlivet i samma moment. Det handlar om att lagstiftaren ska trygga denna rättighet på ett sätt som kan anses godtagbart med hänsyn till de grundläggande fri- och rättigheterna som helhet. Grundlagsutskottet har i sin praxis ansett att det är viktigt med tanke på skyddet för personuppgifter att reglera åtminstone registreringens syfte, innehållet i de registrerade personuppgifterna och tillåtna användningsändamål, vilket inbegriper uppgifternas överlåtbarhet och bevaringstiden för uppgifterna i personregistren, samt den registrerades rättsskydd. Regle-

ringen av dessa faktorer på lagnivå ska dessutom vara omfattande och detaljerad. Enligt grundlagsutskottets avgörandepraxis kan dessa aspekter tillämpas på regleringen av användningen av personuppgifter även ur ett mer allmänt perspektiv.

En målsättning med propositionen är att förtydliga och förenkla bestämmelserna om behandling av personuppgifter inom polisväsendet med beaktande av de anmärkningar om den gällande lagens struktur och innehåll som framgår av förvaltningsutskottets betänkande (FvUB 26/2013). Problemen med den gällande lagens struktur är till stor del en följd av att lagen har ändrats i flera etapper utan att ändringarnas lagstiftningstekniska konsekvenser har kunnat bedömas grundligt ur ett helhetsperspektiv. Det har också ansetts att lagen delvis är komplicerad och svår att tolka för de polisenheter som tillämpar den. Den största ändringen som föreslås gäller lagstiftningstekniken, och syftet med denna ändring är att lagen ska bli lättare att tillämpa. En annan målsättning med propositionen är att iaktta de krav på en detaljerad och noggrant avgränsad lagstiftning som framställts i tolkningspraxisen när det gäller grundlagen och människorättskonventionerna.

I det 1:a lagförslaget i propositionen tas de ovannämnda kraven i beaktande samtidigt som lagstiftningen ändras så att den möter de centrala behov i fråga om personuppgiftsbehandling och dataskydd som föranletts av förändringarna i omvärlden och polislagstiftningen. Dessa förändringar har lett till ett ökat behov av att säkerställa att personuppgifter som fås genom informationsutbyte, kriminalunderrättelseinhämtning och informationsinhämtning som baserar sig på öppna källor behandlas på behörigt sätt. Avsikten är att de nämnda kraven ska beaktas också i innehållet i det 2:a lagförslaget i propositionen till den del lagstiftningen för genomförande av PNR-direktivet måste samordnas med dataskyddsbestämmelserna och kraven på skyddet för de grundläggande fri- och rättigheterna.

3.2 Alternativ

Registerbaserad reglering och reglering som utgår från behandlingsändamålen

Fördelen med registerbaserad reglering kan anses vara att den när det gäller reglering av personuppgiftsbehandling är tydlig, noggrant avgränsad och detaljerad på det sätt som grundlagsutskottet förutsätter. Av den gällande lagens bestämmelser om informationssystemen framgår det i detalj vilka uppgifter som får registreras i varje informationssystem. Grundlagsutskottet hade inget att anmärka på i fråga om det förslag som lades fram i samband med de föregående lagändringarna, nämligen att den kategori av personer och de uppgiftsinnehåll som omfattas av 2 § 2 mom. i den gällande lagen till vissa delar ska utökas (GrUU 18/2012 rd). Däremot påpekade utskottet att formuleringen i den föreslagna bestämmelsen avvikande från den då gällande bestämmelsen innebar att det i sista hand är myndigheten som i hög grad själv definierar innehållet i de personuppgifter som registreras. Grundlagsutskottet hade i ett tidigare utlåtande uttryckligen konstaterat att det inte finns någon sådan risk, eftersom det anges tillräckligt noggrant vilka uppgifter som får registreras i informationssystemen (GrUU 51/2002 rd, s. 2). Grundlagsutskottet har i samband med behandlingen av de gällande paragraferna bl.a. fäst vikt vid registreringen av uppgifter som är nödvändiga för en persons egen säkerhet eller en myndighets säkerhet i arbetet (säkerhetsuppgifter). Utskottet påpekar i sitt utlåtande att bestämmelsen åtminstone delvis reglerar så kallade känsliga uppgifter, varför det är särskilt viktigt att bestämmelsen på ett uttömmande sätt anger det tillåtna innehållet i uppgifter som får registreras. Utskottet anser det vara viktigt att innehållet i de uppgifter som gäller de registrerades identitet regleras i detalj. (GrUU 18/2012 rd)

När det är fråga om registerbaserad reglering är det också tydligt för den polis som behandlar personuppgifter var personuppgifterna ska registreras. Problemen med otillräckligt avgränsad reglering i den gällande lagen gäller snarare bestämmelserna om utlämnande av uppgifter och

förenlig behandling av personuppgifter, som också delvis överlappar med den nya EU-lagstiftningen om dataskydd. Den gällande lagen innehåller bestämmelser om för vilka andra ändamål personuppgifter kan lämnas ut, men dessa bestämmelser har under beredningen bedömts vara något bristfälliga. Samtidigt anges det inte exakt i lagen ur vilka informationssystem eller för vilka behandlingsändamål registrerade personuppgifter får lämnas ut.

När det gäller exakthet och noggrann avgränsning finns det i praktiken inga betydande skillnader mellan registerbaserad reglering och sådan reglering som utgår från behandlingsändamålen. Det krav på exakthet och noggrann avgränsning i anslutning till bestämmelserna om personuppgiftsbehandling som framgår av grundlagsutskottets tolkningspraxis bedöms vara möjligt att uppfylla genom både registerbaserad reglering och behandlingsändamålsbaserad reglering. En reglering som utgår från behandlingsändamålen är emellertid till sin natur en enklare lösning. I samband med lagberedningen har det bedömts i vilken mån det är möjligt att förenkla bestämmelserna i lagen och samtidigt ändå säkerställa att regleringen är tillräckligt noggrant avgränsad och detaljerad. Fördelen med en reglering som utgår från behandlingsändamålen har ansetts vara att det på så sätt inte uppstår ett behov av att ändra lagstiftningen varje gång som ändringar måste göras i informationssystemen. Även den nya EU-lagstiftningen om dataskydd och bestämmelserna om personuppgiftsbehandling i Europolförordningen grundar sig på behandlingsändamålen. Vidare ska det noteras att EU-lagstiftningen om dataskydd förutsätter att kraven i lagstiftningen ska gälla all behandling av personuppgifter oberoende av vilken behandlingsteknik och teknologi som använts.

En reglering som grundar sig på ändamålsbunden personuppgiftsbehandling bedöms förtydliga indelningen av ändamålen med personuppgiftsbehandlingen enligt dataskyddsförordningen och dataskyddsdirektivet i ursprungliga behandlingsändamål och sådan personuppgiftsbehandling som är förenlig med dessa. En sådan reglering preciserar också regleringens förhållande till å ena sidan dataskyddsförordningen och å andra sidan dataskyddsdirektivet med beaktande av deras olika tillämpningsområden, som emellertid i fråga om vardera rättsakten baserar sig på behandlingsändamål. I EU-lagstiftningen om dataskydd föreskrivs det inte heller om något krav på nationell lagstiftning om personregister, utan det fastställs att personuppgiftsbehandlingen ska vara lagenlig och bygga på en godtagbar rättsgrund.

I de bestämmelser som utgår från behandlingsändamålen måste det ovannämnda kravet på exakthet och noggrann avgränsning som framgår av grundlagsutskottets tolkningspraxis dock beaktas. En förenklad reglering ökar behovet av anvisningar från den personuppgiftsansvarige. Med tanke på kravet på en noggrant avgränsad reglering bör det observeras att dessa anvisningar ändå inte får komplettera registrens uppgiftsinnehåll, utan de ska precisera hur bestämmelserna ska tolkas. De behandlingsändamål som definieras i EU-lagstiftningen om dataskydd förutsätter också i viss mån en precisering av vilka ärenden som hänför sig till dataskyddsdirektivets tillämpningsområde och vilka ärenden som hör till den direkt tillämpliga dataskyddsförordningen. Detta ska framgå på lagnivå. I fråga om dataskyddsdirektivet gäller det att observera att den miniminivå för dataskyddet som fastställs i direktivet inte får försvagas. Nivån på dataskyddet får enbart skärpas. Även i fråga om dataskyddsförordningens tillämpningsområde gäller det att i bestämmelserna säkerställa att sådan personuppgiftsbehandling som hör till förordningens tillämpningsområde bygger på en godtagbar rättsgrund och att inskränkningar i en registrerads rättigheter är nödvändiga och proportionerliga.

En eventuell nackdel med en reglering som utgår från behandlingsändamålen kan anses vara att lagens bestämmelser ur slutanvändarens synvinkel inte tydligt anger i vilka register eller delar av ett informationssystem personuppgifterna ska registreras, vilket kan öka risken för fel. Den nya regleringen kräver att den personuppgiftsansvarige tillhandahåller anvisningar och utbildning. Samtidigt krävs detta i samband med lagstiftningsreformen oavsett vilken regleringslösning som väljs. När det gäller förenlig behandling av personuppgifter är det exempel-

vis nödvändigt att veta i vilka delar av ett informationssystem eller i vilka register sökningar får göras. Med tanke på kraven i bestämmelserna om de grundläggande fri- och rättigheterna och dataskyddslagstiftningen ska det noteras att inte heller s.k. massökningar är tillåtna, vilket innebär att användarna av registren måste instrueras bl.a. om hur sökningarna ska begränsas. I samband med en övergång till behandlingsändamålsbaserad reglering måste också bestämmelserna om utlämnande av personuppgifter, tidsfrister för radering av personuppgifter och den registrerades rättigheter bedömas på nytt, och då gäller det att tillräckligt noggrant knyta bestämmelserna till behandlingsändamålen.

Bestämmelser om behandlingen av passageraruppgifter

När det gäller genomförandet av PNR-direktivet har två regleringslösningar bedömts i samband med lagberedningen. En första lösning som bedömts och som är förenlig med den gällande lagen är att i det 1:a lagförslaget genomföra endast de bestämmelser i PNR-direktivet som gäller personuppgiftsbehandling antingen som en del av de övriga behandlingsändamålen eller som ett separat kapitel. En faktor som talar för att bestämmelserna ska tas in i det 1:a lagförslaget är att alla ändamål för polisens personuppgiftsbehandling finns samlade i samma kapitel eller lag. Detta är också ett tydligt alternativ, eftersom det enligt direktivet är tillåtet att jämföra passageraruppgifter i samband med brottmål. En nackdel med denna regleringslösning är att inrättandet av en sådan enhet för passagerarinformation som krävs enligt direktivet, de befogenheter som fastställts för denna samt vissa andra krav enligt direktivet förutsätter att dessa beaktas separat i den övriga lagstiftningen. Vidare ska bestämmelserna om behandling av personuppgifter i större omfattning separat också tas in i lagstiftningen om Tullen och Gränsbevakningsväsendet.

Ett andra regleringsalternativ som analyserats är en separat genomförandelag. Om direktivets genomförandebestämmelser om personuppgifter tas in i det 1:a lagförslaget blir regleringen splittrad på det sätt som beskrivits ovan. Fördelen med en separat lag om genomförande av direktivet är att regleringen blir enhetligare när det gäller den behandling av passageraruppgifter som utförs av polisen, Tullen och Gränsbevakningsväsendet. När lagstiftningen ska tillämpas av enheten för passagerarinformation är det dessutom tydligare om alla genomförandebestämmelser finns samlade i en enda lag. Dessutom kan också de bestämmelser om inrättande av en enhet för passagerarinformation och befogenhetsbestämmelser som krävs enligt direktivet samt rättsskyddsaspekterna beaktas till alla delar i genomförandelagen. Denna regleringslösning kräver förutom en genomförandelag endast enskilda lagändringar som bifogade lagar.

Bestämmelser om skyddspolisen

Beträffande skyddspolisen har två alternativ undersökts: för det första att bevara den regleringslösning som används i den gällande lagen och ta in den i det 1:a lagförslaget, varvid bestämmelserna utgör en del av polisens övriga ändamål med behandlingen av personuppgifter, och för det andra att ta in bestämmelserna i ett särskilt kapitel. Att bevara den regleringslösning som används i den gällande lagen är möjligt i det fallet att man i det 1:a lagförslaget håller fast vid den registerbaserade regleringen, varvid skillnaden jämfört med övrig personuppgiftsbehandling förblir tydlig. Med beaktande av ett av de viktigaste förslagen i propositionen är det till denna del motiverat att för skyddspolisens del överföra alla bestämmelser som gäller personuppgiftsbehandling till ett särskilt kapitel för tydlighetens skull.

Vidare har regleringslösningen för skyddspolisens del bedömts med avseende på de allmänna bestämmelserna om personuppgiftsbehandling. Inom lagberedningen har man bedömt dels vilka möjligheter det finns att bereda en separat lag om skyddspolisen, dels vilken nationell lag som alternativt kan tillämpas på behandlingen av personuppgifter vid skyddspolisen. Ett faktum som talar för ett separat lagförslag är det att när skyddspolisen behandlar personupp-

gifter för att utföra sina uppgifter, dvs. för att skydda den nationella säkerheten, omfattas denna personuppgiftsbehandling inte av EU-rätten. Därmed är även strävan efter att utvidga den nationella genomförandelagstiftningen så att den omfattar skyddspolisens personuppgiftsbehandling förknippad med vissa utmaningar. Nationell säkerhet är ett område som i fördraget om Europeiska unionen faller utanför EU:s behörighet. Av denna anledning måste det i vilket fall som helst genom nationell lagstiftning föreskrivas om personuppgifter som ska behandlas på grundval av nationell säkerhet. EU:s dataskyddsdirektiv och dataskyddsförordning utesluter uttryckligen ur sitt tillämpningsområde sådan personuppgiftsbehandling som hänför sig till nationell säkerhet. EU:s dataskyddsdirektiv förhindrar dock inte att lagstiftningen för dess genomförande utsträcks till att gälla sådan personuppgiftsbehandling som hänför sig till verksamhet som helt och hållet faller utanför EU-rättens tillämpningsområde. Den gällande personuppgiftslagen, genom vilken det personuppgiftsdirektiv som nu ska upphävas har genomförts, gäller all behandling av personuppgifter på nationell nivå, inklusive den behandling som utförs av skyddspolisen med de begränsningar som anges i den gällande personuppgiftslagen för polisväsendet. Strävan efter att säkerställa en enhetlig dataskyddsreglering talar för att tillämpningsområdet för lagen för genomförande av dataskyddsdirektivet ska utvidgas till att gälla även den personuppgiftsbehandling som utförs av skyddspolisen.

3.3 De viktigaste förslagen

Personuppgiftsbehandling som utgår från behandlingsändamålen

EU:s dataskyddsdirektiv förutsätter att medlemsstaterna i sin lagstiftning, där det föreskrivs om uppgiftsbehandling som hör till direktivets tillämpningsområde, ska precisera åtminstone målsättningarna för behandlingen, vilka personuppgifter som ska behandlas och ändamålen med behandlingen. Även dataskyddsförordningen kräver nationell kompletterande lagstiftning i situationer där behandlingen av personuppgifter grundar sig på den personuppgiftsansvariges lagstadgade skyldighet eller där behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller för den personuppgiftsansvariges myndighetsutövning. Valet mellan en registerbaserad eller en ändamålsbaserad regleringslösning i den nationella lagstiftningen begränsas inte i något avseende av EU-lagstiftningen om dataskydd. Det föreslås att den gällande lagens 2 kap. 2, 3 och 4 §, som gäller riksomfattande informationssystem, samt bestämmelserna om polisens övriga personregister i 6 § ersätts med bestämmelser om ändamålen med behandlingen av personuppgifter. Enligt förslaget ska bestämmelserna om uppgiftsbehandlingen när det gäller behandlingsändamålen vara mer exakta, så att principen om ändamålsbegränsning uppfylls konsekvent i polisens olika informationssystem.

När det gäller frågan vilka uppgifter som får registreras i informationssystemen har man med tanke på lagens struktur och tydlighet och för att undvika kontinuerliga ändringsbehov undersökt möjligheten att slopa de detaljerade förteckningarna över uppgifternas innehåll. Alternativet att slopa de detaljerade förteckningarna förutsätter att målet med registreringen av personuppgifter och personuppgiftsbehandlingens syften framgår tillräckligt exakt av bestämmelserna om behandlingsändamål. Det föreslås dock att det i bestämmelserna om ursprungliga ändamål med behandlingen av personuppgifter alltjämt ska föreskrivas om olika kategorier av personer. I regeringspropositionen fästs särskild vikt vid det i dataskyddsdirektivet angivna kravet på att uppgifter som rör olika kategorier av personer vid behov och i den mån det är möjligt ska separeras från varandra.

Med tanke på grundlagsutskottets anmärkningar på de gällande bestämmelserna är det viktigt att inte bara de olika kategorierna av personer som får registreras utan också de grundläggande uppgifterna om personernas identitet samt övriga personuppgifter som får behandlas anges tillräckligt detaljerat även i den ändamålsbaserade regleringen. Avvikande från den gällande lagen föreslås det att de grundläggande uppgifter om en person som får behandlas ska regleras

i en paragraf (2 kap. 1 §), som gäller alla ursprungliga behandlingsändamål enligt 2 kap. I den föreslagna 2 kap. 2 § ska det på motsvarande sätt föreskrivas om sådana personuppgifter som hänför sig till ett aktuellt ärende och som till den del det är nödvändigt får behandlas för respektive ursprungligt behandlingsändamål enligt 2 kap.

Strävan har varit att i de föreslagna bestämmelserna undvika onödiga överlappningar med den allmänt tillämpliga dataskyddslagstiftningen och onödiga detaljer. Det 1:a lagförslaget ska inte innehålla sådana bestämmelser som tas in i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Till vissa delar har det ändå bedömts vara nödvändigt att i personuppgiftslagen för polisväsendet precisera bestämmelserna om allmän personuppgiftsbehandling med beaktande av den betydelse de har för integritetsskyddet. Grundlagsutskottet har t.ex. fäst vikt vid att behandlingen av känsliga uppgifter berör själva kärnan i skyddet för personuppgifter, som utgör en del av privatlivet, och att bestämmelser som tillåter behandling av sådana uppgifter därför måste vara exakta (GrUU 25/1998 rd, s. 3, GrUU 51/2002 rd). Grundlagsutskottet har också ansett att exakta bestämmelser om behörighet att behandla känsliga uppgifter måste tas in i lagen när det gäller sådan personuppgiftsbehandling som utförs av polisen, eftersom personuppgiftslagen är en allmän lag och därför inte ger sådan behörighet (GrUU 51/2002 rd). Även EU-lagstiftningen om dataskydd förutsätter preciserande lagstiftning och särskilda skyddsåtgärder när det gäller behandling av känsliga personuppgifter. Det 1:a lagförslaget i propositionen innehåller förutom bestämmelser om personuppgifternas innehåll i 2 kap. även särskilda bestämmelser om skydd av känsliga personuppgifter (9 kap. 1 §). På behandlingen av känsliga personuppgifter tillämpas också de allmänna villkor för behandling som anges i dataskyddsförordningen och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning

Enligt förslaget ska den gällande lagens 4 §, som gäller informationssystemet för misstänkta, ersättas med en ändamålsbunden bestämmelse om personuppgiftsbehandling som anknyter till kriminalunderrättelseinhämtning. Informationssystemet för misstänkta är enligt 4 § i gällande lag ett personregister som är avsett för polisens riksomfattande bruk och förs med hjälp av automatisk databehandling. Informationssystemet kan innehålla information som för skötseln av uppgifter enligt 1 kap. 1 § i polislagen inhämtats genom kriminalunderrättelseverksamhet, observation eller iakttagelser och som gäller personer som skäligen kan misstänkas 1) göra eller ha gjort sig skyldiga till ett brott på vilket kan följa fängelse, eller 2) medverka eller ha medverkat till ett brott på vilket kan följa fängelse i mer än sex månader, eller till straffbart bruk av narkotika. Av 4 § framgår också vilka uppgifter som ska antecknas i registret. Endast polispersonal som förordnats till kriminalunderrättelse-, brottsanalys- och observationsuppgifter samt de kontaktpersoner som polisen sänt utomlands har med stöd av 4 § genom teknisk anslutning tillgång till informationssystemet för misstänkta. Av lagstiftningen framgår att det genom teknisk anslutning är möjligt att lämna ut uppgifter ur informationssystemet för misstänkta även till Gränsbevakningsväsendet och Tullen. Användningsrätt till informationssystemet för misstänkta har beviljats cirka 1 400 personer, av vilka cirka 1 100 är poliser.

Den föreslagna paragrafen om behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning har formulerats med beaktande av förvaltningsutskottets ovan angivna anmärkningar i fråga om informationssystemet för misstänkta. Paragrafen innehåller en uttömmande förteckning över de kategorier av personer som får registreras i informationssystemet. Särskilda behandlingskriterier ska fastställas för registrering av uppgifter och övrig personuppgiftsbehandling som hänför sig till dessa kategorier av personer. Uppgifter om en person som gör eller gjort sig skyldig till brottslig verksamhet får behandlas under förutsättning att personen i fråga kan antas ha samband med ett brott eller brottslig verksamhet. Uppgifter om

andra misstänkta personer än sådana som misstänks ha gjort sig skyldiga till egentlig brottslig verksamhet kan få behandlas, men tröskeln är högre för sådan behandling av uppgifter.

På samma sätt som i den gällande lagen föreslås det att 2 kap. 6 § också ska innehålla bestämmelser om att polisen har rätt att registrera uppgifter om observationer som gjorts av poliser eller uppgifter som anmälts till polisen i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser eller uppträdande i övrigt med fog kan bedömas ha samband med brottslig verksamhet (observationsuppgifter).

När det gäller kriminalunderrättelseinhämtning får även uppgifter som införts i sådana temporära register för brottsanalys som avses i 6 § i den gällande lagen behandlas under de förutsättningar som anges i den föreslagna paragrafen om behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning. Liksom den gällande regleringen om observationsuppgifter är syftet med den föreslagna paragrafen om personuppgifter som anknyter till kriminalunderrättelseinhämtning att i regel undvika att denna typ av personuppgifter förs in i polisenhetsspecifika register eller lagras på polisers databärare som används av andra personer. En utspridd lagring av uppgifter orsakar problem med tanke på övervakningen. Genom den föreslagna regleringen förbättras också möjligheterna att rikta polisens verksamhet och att förebygga och utreda brott. När alla uppgifter som inhämtats genom kriminalunderrättelseverksamhet, observation eller iakttagelser lagras på en lagringsplattform blir det lättare att styra och övervaka personuppgiftsbehandlingen och att skydda uppgifterna, vilket även anses förbättra den registrerades rättsskydd.

Den registrerades rätt till insyn omfattar enligt den gällande lagen varken uppgifter i informationssystemet för misstänkta eller observationsuppgifter. Dataombudsmannen får emellertid på begäran av den registrerade kontrollera att uppgifterna om den registrerade är lagenliga. Det föreslås att den registrerade endast ska ha indirekt rätt till insyn även i fråga om personuppgifter som anknyter till kriminalunderrättelseinhämtning.

Förvaltningsutskottet har tidigare begrundat om det för att säkerställa en effektiv tillsyn borde föreskrivas till exempel om en särskild skyldighet att årligen rapportera om behandlingen av observationsuppgifter till dataombudsmannen. Med beaktande av den korta lagringstid som gäller för observationsuppgifter, den personuppgiftsansvariges skyldigheter enligt personuppgiftslagen, datasekretessmyndigheternas rätt att få information och utföra inspektioner samt med hänsyn till laglighetskontrollen i övrigt har utskottet ansett att tillsynen över behandlingen av observationsuppgifter kan ske på behörigt sätt (FvUB 26/2013 rd). De föreslagna preciserande bestämmelserna om registerföring och tillsyn över registren samt de bestämmelser om personuppgiftsbehandling som allmänt ska tillämpas på övervakningen, och som bygger på EU:s dataskyddsdirektiv, anses uppfylla behoven i anslutning till övervakningen av uppgiftsbehandlingen.

Innehållet i uppgifter som inhämtats genom kriminalunderrättelseinhämtning, observation och iakttagelser har med beaktande av grundlagsutskottets tidigare anmärkningar begränsats i bestämmelsen, så att bara sådana uppgifter får registreras som anknyter till händelser eller personer som utifrån omständigheterna eller en persons hotelser kan bedömas ha samband med brottslig verksamhet. Uppgifter som registreras ska om möjligt åtföljas av en bedömning av uppgiftslämnarens tillförlitlighet och uppgifternas riktighet. Enligt den föreslagna paragrafen om förenlig behandling av personuppgifter får observationsuppgifter inte heller användas i samband med beslut eller utlåtanden som gäller beviljande eller giltighet av ett tillstånd. Vidare får observationsuppgifter endast lagras under en kort tid. Grundlagsutskottet har ansett att den gällande regleringen av observationsuppgifter, i och med att den begränsas på detta sätt i fråga om informationsinnehåll, användningsändamål och förvaringstid, inte blir problematisk med avseende på skyddet för personuppgifter. Med tanke på observationsuppgifternas natur

har grundlagsutskottet ändå ansett det vara viktigt att villkoren för lagring av uppgifter tolkas snävt och i synnerhet så att observationsuppgifter får lagras endast om det finns misstanke om brottslig verksamhet (GrUU 18/2012 rd).

Förenlig behandling av personuppgifter

Den nya EU-lagstiftningen om dataskydd förutsätter att personuppgifter i regel ska behandlas endast för det lagstadgade ändamål för vilket de har samlats in. Dataskyddslagstiftningen möjliggör emellertid behandling av personuppgifter även för andra lagstadgade ändamål, om behandlingen är nödvändigt och proportionell. I dataskyddsdirektivet har principen om förenlig behandling av personuppgifter dock i viss mån skärpts i förhållande till den tidigare EU-regleringen, och även förenlig personuppgiftsbehandling är tämligen strikt bunden till direktivets tillämpningsområde. Med hänsyn till grundlagsutskottets tolkningspraxis är det också viktigt att regleringen är tillräckligt detaljerad och noggrant avgränsad.

Paragrafen om förenlig behandling av personuppgifter motsvarar huvudsakligen 16 och 16 a § i den gällande lagen, men bestämmelserna utvidgas och preciseras till vissa delar. Den viktigaste utvidgningen är det föreslagna 2 kap. 11 § 5 mom., som gäller användning av fingeravtrycksuppgifter som har samlats in med stöd av 131 § i utlänningslagen för andra ändamål än deras ursprungliga ändamål. I nuläget får fingeravtrycksuppgifter som införts i polisens register med stöd av utlänningslagen användas för andra ändamål än de som uppgifterna ursprungligen samlats in för under samma förutsättningar som fingeravtrycksuppgifter i pass. Det föreslås att bestämmelsen om användningen av fingeravtryck som registrerats med stöd av 131 § i utlänningslagen ska utvidgas så att det är möjligt att använda fingeravtryck förutom för förenliga behandlingsändamål som gäller fingeravtrycksuppgifter i pass även för att förebygga, avslöja eller utreda terroristbrott och andra grova brott som avses i Eurodacförordningen (EU) nr 603/2013. En förutsättning för att fingeravtrycksuppgifter ska kunna användas är att det är nödvändigt för identifieringen av en person. På så sätt säkerställs en proportionell personuppgiftsbehandling.

Behandling av personuppgifter vid skyddspolisen

Avvikande från den gällande lagen ska bestämmelserna om behandling av personuppgifter vid skyddspolisen finnas i ett särskilt kapitel. När skyddspolisen behandlar personuppgifter för att utföra sina uppgifter, dvs. för att skydda den nationella säkerheten, omfattas denna personuppgiftsbehandling inte av EU-rätten. Nationell säkerhet är ett område som i fördraget om Europeiska unionen faller utanför EU:s behörighet. Av denna anledning måste det genom nationell lagstiftning föreskrivas om personuppgifter som ska behandlas på grundval av nationell säkerhet. Bortsett från det särskilda kapitlet för behandling av personuppgifter vid skyddspolisen föreslås inga stora principiella ändringar jämfört med den gällande regleringen. Personuppgifter kan precis som nu behandlas på det sätt som uppdraget förutsätter. Därtill föreskrivs det om utlämnande av uppgifter i en separat paragraf. I fråga om lagringstid och inskränkning av den registrerades rätt till insyn föreslås inga ändringar jämfört med den gällande lagen.

I 7 kap. 9 § i det 1:a lagförslaget i propositionen finns emellertid en ny bestämmelse där det föreskrivs om uppdatering av personuppgifter i system med hög informationssäkerhetsnivå som innehåller uppgifter som ska behandlas för att skydda den nationella säkerheten och som därmed är förknippade med särskilda informationssäkerhets- och dataskyddsrisker. Syftet med den föreslagna bestämmelsen är att ge skyddspolisen rätt att uppdatera sitt informationssystem så att inte uppgifter från ett system med högre dataskyddsnivå överförs till ett system med lägre dataskyddsnivå i samband med en förfrågan. Bestämmelsen har ansetts vara nödvändig för att inte skyddspolisen ska äventyra de personers säkerhet som är föremål för informationsinhämtning.

Utnyttjande av passageraruppgiftssamlingar för brottsbekämpning

Enligt PNR-direktivet är lufttrafikföretag skyldiga att, i syfte att bekämpa sådan terrorism och grov brottslighet som avses i direktivet, överföra bestämda passageraruppgifter till de enheter för passagerarinformation som medlemsstaterna inrättat eller utsett. Med passageraruppgiftssamling avses en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt att behandla och kontrollera passagerarens reservationer, t.ex. personens namn, adress och kontaktuppgifter samt uppgifter om betalningssätt.

I Finland utgörs den i direktivet avsedda enheten för passagerarinformation av en enhet som bildats inom den PTG-kriminalunderrättelsestruktur som avses i 5 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009). Enheterna för passagerarinformation analyserar uppgifterna enligt på förhand fastställda kriterier och jämför dem med uppgifter i nationella och internationella databaser som är väsentliga med tanke på bekämpningen av terroristbrott och grov brottslighet. Målet är att identifiera personer som de nationella brottsbekämpande myndigheterna eller Europol behöver utreda ytterligare på grund av att dessa personer kan vara inblandade i sådana terroristbrott eller sådan grov brottslighet som definieras i PNR-direktivet. Om ytterligare undersökningar visar sig vara nödvändiga överför enheten för passagerarinformation uppgifterna till de behöriga myndigheterna i den egna medlemsstaten eller till enheten för passagerarinformation i en annan EU-medlemsstat. Behöriga myndigheter i Finland är polisen, Tullen och gränsbevakningsväsendet. Även Europol har rätt att begära enskilda uppgifter inom ramen för sina arbetsuppgifter och sin behörighet. Passageraruppgifter kan överföras till tredjeländer endast i enskilda fall, och förutom de allmänna villkor som ställs i dataskyddsdirektivet ställer PNR-direktivet särskilda villkor för utlämnandet av uppgifter.

Passageraruppgifterna ska lagras vid enheten för passagerarinformation under en period på fem år. Sex månader efter att uppgifterna överförts till enheten för passagerarinformation ska uppgifterna avidentifieras genom maskering av sådana uppgifter som kan användas för att omedelbart identifiera de passagerare som uppgifterna avser. När denna period på sex månader gått ut får alla passageraruppgifter lämnas ut endast på grundval av en motiverad begäran från polisen, Tullen, gränsbevakningsväsendet eller Europol och ett samtycke från en polisman som hör till befälet.

Medlemsstaterna ska sätta i kraft de bestämmelser som är nödvändiga för att följa direktivet senast den 25 maj 2018. Det 2:a lagförslaget i propositionen ska enligt förslaget innehålla de bestämmelser om överföring, behandling, lagring, utlämnande och radering av passageraruppgifter, som krävs för genomförandet av direktivet.

4 Propositionens konsekvenser

4.1 Ekonomiska konsekvenser

Konsekvenserna av det 1:a lagförslaget i propositionen drabbar huvudsakligen privatpersoner i och med att personuppgiftsbehandling i väsentlig grad anknyter till bestämmelserna om de grundläggande fri- och rättigheterna och i synnerhet integritetsskyddet. Lagförslagets ekonomiska konsekvenser rör emellertid huvudsakligen myndigheter, dvs. förutom den personuppgiftsansvarige alla polisenheter som behandlar personuppgifter. Europeiska kommissionens ursprungliga konsekvensbedömning och de bedömningar som gjorts av de arbetsgrupper som bereder genomförandet av dataskyddslagstiftningen avviker från varandra. Exempelvis den arbetsgrupp som bereder genomförandet av EU:s allmänna dataskyddsförordning (TATTI) konstaterar på s. 133 i sitt betänkande att bestämmelserna i den allmänna dataskyddsförordningen orsakar många typer av kostnader såväl för tillsynsmyndigheterna som för de person-

uppgiftsansvariga och personuppgiftsbiträdena inom både den privata och den offentliga sektorn. Däremot har det i Europeiska kommissionens konsekvensbedömning av EU:s dataskyddslagstiftning ursprungligen bedömts att en ny, enhetligare reglering inte får betydande ekonomiska konsekvenser, och inget tyder på att den nya regleringen kommer att kräva tilläggsresurser.

En omständighet som minskar de direkta ekonomiska konsekvenserna av skyldigheten att utnämna ett dataskyddsombud är det att flera personuppgiftsansvariga kan utnämna ett gemensamt dataskyddsombud, och kravet gäller exempelvis inte polisinrättningarna. Samtidigt har riksdagen särskilt uppmanat polisen att utveckla övervakningen av sin personuppgiftsbehandling, och de personuppgiftsansvariga kan således om de så önskar även utnämna enhetsspecifika dataskyddsombud. Detta kan få indirekta ekonomiska konsekvenser. EU-regleringen och det 1:a lagförslaget har emellertid också andra direkta och indirekta ekonomiska konsekvenser. Lagförslaget kompletterar EU-lagstiftningen om dataskydd och den allmänt tillämpliga lagstiftningen om genomförandet av denna, vars ekonomiska och administrativa konsekvenser till stor del konkretiseras i samband med tillämpningen av bestämmelserna i lagförslaget. De direkta ekonomiska konsekvenserna orsakas av de krav i dataskyddsförordningen och dataskyddsdirektivet som måste uppfyllas och av vissa nya behandlingsändamål som ingår i det 1:a lagförslaget och som i praktiken innebär antingen att ett nytt personregister måste inrättas eller att innehållet i ett befintligt register måste utvidgas. Som indirekta ekonomiska konsekvenser kan betraktas behoven att utveckla övervakningen och informationssystemen även i andra avseenden så att dataskydds- och informationssäkerhetsnivån förbättras. De nya skyldigheterna i anslutning till behandlingen av personuppgifter uppfylls i regel genom befintliga resurser, med undantag av de skyldigheter som följer av genomförandet av EU-lagstiftningen om dataskydd, som till vissa delar kräver tilläggsfinansiering.

De ekonomiska konsekvenserna av propositionen kan uppskattas i euro endast när det gäller konsekvenserna för statsfinanserna och informationssystemen. I övrigt saknas det en tillräcklig statistisk grund som skulle möjliggöra en exakt beräkning av kostnadseffekterna, och därför har bedömningen av de ekonomiska konsekvenserna genomförts som en kvalitativ bedömning främst med hjälp av expertbedömningar som fåtts av personuppgiftsansvariga, systemexperter och dataskyddsexperter. När det gäller konsekvenserna för företag har man beträffande behandlingen av passageraruppgifter utnyttjat Europeiska kommissionens konsekvensbedömning, som hänför sig till kommissionens förslag om PNR-direktivet, och den motsvarande konsekvensbedömningen av EU-lagstiftningen om dataskydd. Med beaktande av de ändringar som gjorts i bestämmelserna under förhandlingarna om dessa rättsakter har strävan varit att till kompletterande delar bedöma konsekvenserna för företag i ljuset av nuläget och genom att utnyttja remissförfarandet. Med avseende på sådan personuppgiftsbehandling som sker i EU-medlemsstaterna leder det 1:a lagförslaget inte till betydande ändringar i bestämmelsernas innehåll jämfört med nuläget.

Konsekvenser för företag

De ekonomiska konsekvenser för företag som följer av det 1:a lagförslaget gäller främst enskilda företagsgrupper, eftersom en del av de föreslagna uttryckliga bestämmelserna i viss mån kan uppskattas leda till att dessa företag dels oftare lämnar ut personuppgifter direkt, dels får fler begäranden om utlämnande av personuppgifter.

När det gäller behandling av personuppgifter i syfte att förebygga, utreda och avslöja brott hänför sig konsekvenserna för företag till enskilda uttryckliga bestämmelser i det 1:a lagförslaget, som gör det möjligt att på grundval av vissa kriterier lämna ut personuppgifter till ett privat företag eller en privat sammanslutning. Den föreslagna bestämmelsen om brådskande direkt utlämnande av uppgifter i enskilda fall grundar sig på motsvarande bestämmelse i lagen

om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, som gäller utlämnande av personuppgifter till mottagare i tredjeländer. Någon sådan uttrycklig bestämmelse finns inte i den gällande lagen, men direkta överföringar av uppgifter är med stöd av det gällande dataskyddsrambeslutet möjliga mellan EU-medlemsstater. Denna typ av direkt utlämnande av personuppgifter har också genomförts.

Europeiska kommissionen har i sin egen konsekvensbedömning på EU-nivå poängterat att en enhetligare och mer detaljerad reglering av personuppgiftsbehandling i anslutning till brottmål i alla EU-medlemsländer kommer att förtydliga rättsläget och öka företagens förtroende för polisens behandling av personuppgifter. Kommissionen anser att detta har betydelse särskilt i situationer där en brottsbekämpande myndighet direkt kontaktar företag som verkar inom EU för att få eller lämna ut personuppgifter när det gäller tillhandahållande av gränsöverskridande tjänster. På motsvarande sätt ökar den allmänt tillämpliga dataskyddsförordningen myndigheternas förtroende för den behandling av personuppgifter som företagen utför. Även om det redan med stöd av den gällande EU-regleringen är möjligt för polisen att direkt lämna ut personuppgifter till företag som verkar inom EU kan mer detaljerade och enhetligare bestämmelser uppskattas få en positiv effekt såtillvida att polisen oftare än tidigare utnyttjar sina rättigheter att lämna ut personuppgifter till företag i en brådskande situation när detta är nödvändigt för att förebygga, utreda eller avslöja ett brott. Till den del det handlar om informationsinhämtning från inhemska företag motsvarar bestämmelserna i det 1:a lagförslaget huvudsakligen den gällande regleringen, varför lagförslaget till denna del inte antas påverka företagens verksamhet i någon betydande grad. Den förenhetligade EU-regleringen kan dock uppskattas få indirekta ekonomiska och personalrelaterade konsekvenser för inhemska företag i sådana situationer där de brottsbekämpande myndigheterna i en annan EU-medlemsstat oftare än tidigare utnyttjar sina direkta möjligheter att lämna ut och inhämta information.

Den gällande EU-lagstiftningen om dataskydd möjliggör inte uttryckligen utlämnande av personuppgifter till ett privat företag eller en privat sammanslutning i ett tredjeland, utan överföringarna av personuppgifter ska ske mellan behöriga myndigheter. Överföringar av personuppgifter mellan behöriga myndigheter ska vara huvudregeln även enligt den nya dataskyddslagstiftningen. När personuppgifter behöver inhämtas från ett företag som verkar i ett tredjeland ska polisen i regel alltjämt utnyttja förfarandet med begäran om rättshjälp eller handräckning. Det föreslås emellertid att lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten avvikande från den gällande lagstiftningen ska innehålla en bestämmelse om att polisen eller någon annan i dataskyddsdirektivet avsedd behörig myndighet utifrån vissa kriterier, i synnerhet i brådskande situationer, kan lämna ut personuppgifter direkt till en personuppgiftsansvarig i ett tredjeland. Eftersom denna bestämmelse har fogats till direktivförslaget under arbetsgruppsbehandlingen omfattar kommissionens konsekvensbedömning inte dess ekonomiska eller andra konsekvenser. Bestämmelsen ska i praktiken tillämpas tillsammans med bestämmelserna i personuppgiftslagen för polisväsendet. Det kan exempelvis handla om att polisen begär att personuppgifter eller meddelanden som företaget har i sin besittning ska frysas, vilket påverkar företagets verksamhet som personuppgiftsansvarig. Trots att utlämnandet av personuppgifter begränsas till sådana uppgifter som är nödvändiga för att förebygga, utreda eller avslöja brott kan de nya bestämmelserna få direkta ekonomiska konsekvenser för utländska företag till den del polisen i och med denna uttryckliga bestämmelse oftare väljer att kontakta företagen direkt. Dessa konsekvenser kan också omspänna informationssystemen. En del företag har emellertid redan etablerad praxis för lagring av personuppgifter, och i deras fall blir de ekonomiska konsekvenserna ringa eller måttliga.

De största konsekvenserna för företagen följer av det 2:a lagförslaget. PNR-direktivets ekonomiska konsekvenser för lufttrafikföretagen har bedömts i en U-skrivelse som statsrådet överlämnade till riksdagen i samband med beredningen av direktivet (U 66/2010 rd) och i

kompletterande skrivelser. Konsekvensbedömningen i denna proposition bygger också framför allt på Europeiska kommissionens konsekvensbedömning, som omspänner hela EU, (SEC(2011) 132 final). Kommissionen har hört ett antal intressentgrupper, inklusive medlemsstaternas dataskyddsmyndigheter, Europeiska datatillsynsmannen samt lufttrafikföretagens takorganisationer (AEA, ATA, IACA, ERA och IATA). Av dessa har IATA och EAA kritiserat främst den decentraliserade informationssystemslösning som kommissionen föreslagit och den relaterade modellen som bygger på en teknisk anslutning (push). Organisationerna önskar att lufttrafikföretagen själva ska få välja vilket sätt eller vilken metod de vill utnyttja för att överföra information. Denna valfrihet kan de facto uppskattas orsaka mindre ekonomiska konsekvenser för företagen i det fall att det förbättrar deras möjligheter att anpassa sina befintliga informationssystem till informationsöverföringen. Samtidigt kan det medföra fler direkta ekonomiska konsekvenser för myndigheternas informationssystem.

I ljuset av denna kritik har kommissionen justerat sin konsekvensbedömning bland annat i fråga om konsekvenserna för företag. Kommissionen har i sin konsekvensbedömning fäst vikt vid att endast lufttrafikföretagen samlar in heltäckande passageraruppgifter. Bara en del av de företag som idkar järnvägstrafik och sjöfart samlar systematiskt in denna typ av uppgifter, och de har lämnats utanför direktivförslaget. Med tanke på att lufttrafikföretagen redan samlar in passageraruppgifter kan konsekvenserna av det 2:a lagförslaget enligt kommissionens bedömning till denna del inte anses bli särskilt betydande. Samtidigt har antalet flygpassagerare ökat under de senaste åren, och i motsats till den befintliga lagen innebär det 2:a lagförslaget att passageraruppgifter ska överföras systematiskt till polisen. I samband med lagberedningen har det uppskattats att detta kommer att påverka lufttrafikföretagens informationssystemslösningar och deras administrativa börda.

Att fullgöra skyldigheterna enligt direktivet och det 2:a lagförslaget leder till direkta ekonomiska konsekvenser för lufttrafikföretagen, inklusive konsekvenser för informationssystemen och personalkostnader. I en undersökning som offentliggjorts år 2009 på grundval av en anbudsbegäran från kommissionen presenteras en uppskattning av kostnaderna för projektet på EU-nivå:

Kostnader som orsakas alla trafikföretag (sammanlagt i euro)

Kostnader för inrättande - anbudsförfarande (engångskostnader):

- 100 000 euro x 120 trafikföretag inom EU: 12 000 000

- 100 000 euro x 80 trafikföretag utanför EU: 8 000 000

Fem års amorteringstid: 4 000 000

Överföringskostnader – anbudsförfarande x 2/passagerare (återkommande):

- 33 500 euro/flygbolag per år x 120 trafikföretag x 3 anslutningar

x 2 överföringar (push): 24 120 000

Personal- och driftskostnader (återkommande): 6 240 000

Enligt kommissionen har de kostnader för inrättandet av EU:s PNR-system som år 2009 uppskattades för myndigheternas del minskat, medan de kostnader som orsakas trafikföretagen har ökat jämfört med kalkylerna från år 2007. Kommissionen har beräknat att de verkliga kostnaderna ligger någonstans mellan dessa siffror och att åtminstone trafikföretagens kostna-

der ligger närmare kalkylerna från år 2007, som bygger direkt på de marknadspriser som trafikföretagen uppgav. Vidare har kommissionen konstaterat att även om de mycket höga kostnadskalkylerna från år 2009 skulle visa sig bli verklighet och trafikföretagen beslutar sig för att överföra sina kostnader på passagerarna, innebär detta en extra kostnad på mindre än 0,10 euro per biljett. De kostnader som orsakas lufttrafikföretagen uppskattades i samband med beredningen av direktivet uppgå till 0,10–0,20 euro/biljett, vilket är en något högre uppskattning än den som gjordes år 2009 (kompletterande U-skrivelse 17.11.2015, promemoria SM2015-00271). Eftersom de tekniska lösningar som påverkar kostnaderna i det skedet delvis ännu inte hade slagits fast, var det inte möjligt att göra någon noggrannare analys. Det finns inte heller någon sådan bedömning att tillgå som skulle visa på vilket sätt regleringen påverkar den ställning som företag som verkar på EU:s inre marknad har i förhållande till företag på den internationella marknaden (flygtrafik över EU:s yttre gränser).

Lufttrafikföretagen orsakas också i viss mån en extra administrativ börda när det gäller att iaktta de skyldigheter som följer av PNR-direktivet och dataskyddslagstiftningen i behandlingen av personuppgifter. Jämfört med den rätt att få information av trafikföretag som polisen har enligt den gällande personuppgiftslagen för polisväsendet innebär det 2:a lagförslaget för lufttrafikföretagens del en mer systematisk och storskalig behandling av personuppgifter, och företagen måste använda en viss typ av teknisk lösning för överföringen av uppgifter. Med tanke på de krav som EU:s nya dataskyddsförordning ställer på de personuppgiftsansvariga vid behandling av personuppgifter kan ett storskaligt utlämnande av uppgifter och det skydd av personuppgifter som detta kräver medföra även en stor administrativ börda för lufttrafikföretagen. Samtidigt är syftet att genom enhetliga tekniska lösningar minska den administrativa bördan för både företagen och myndigheterna.

Kommissionen har också bedömt kostnadseffekterna av olika tekniska lösningar för utlämnande av uppgifter och gjort en jämförelse mellan de s.k. push- och pullmetoderna. Enligt kommissionens utredning medför utlämnandet av passageraruppgifter stora kostnadseffekter för lufttrafikföretagen, och push-metoden leder till avsevärt större kostnadseffekter eftersom lufttrafikföretagen blir tvungna att betala överföringskostnaderna för varje överföring av information. Hur stora kostnader som uppstår för lufttrafikföretagen beror också på det enskilda företagets storlek och mängden flygresor som det opererar. Samtidigt har kommissionen bedömt att lufttrafikföretagen med hjälp av denna metod för utlämnande av uppgifter bättre kan övervaka utlämnandet av personuppgifter och säkerställa att personuppgifterna skyddas på behörigt sätt, och kommissionen har därför beslutat att föreslå push-metoden som teknisk lösning. Lufttrafikföretagen orsakas också kostnader på grund av att informationssystemen ska ändras och det tar tid innan systemen kan tas i bruk. För att lufttrafikföretagen ska kunna lämna ut passageraruppgifter med hjälp av en direktivenlig teknisk lösning måste de genomföra de dataformat och krypteringsmetoder som krävs och bygga upp förbindelser för utlämnandet av uppgifter till alla medlemsstater till vilka de har lufttrafik. Exakt vilka konsekvenser dessa tekniska ändringar får varierar från ett företag till ett annat.

När det gäller personuppgiftsbehandling i anslutning till tillståndsärenden ges det i lagförslaget akt på att polisen för att kunna sköta sin lagstadgade uppgift behöver behandla sådana personuppgifter som härrör från privata företag, särskilt fotografier för sådana ändamål som tjänar polisens tillståndsförvaltning. I förslaget beaktas också att personuppgifter som behandlas av polisen i vissa situationer får lämnas ut till privata företag. Sådana situationer uppstår särskilt när tillståndshandlingar ska levereras till en enskild person via ett privat företag, när uppgifter om vapentillstånd ska kontrolleras i företag som säljer vapen och när tillståndshandlingars giltighet ska kontrolleras exempelvis i banker och i andra organisationer enligt lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) som erbjuder en identifieringstjänst. Syftet med lagförslaget är att säkerställa att personuppgifter behandlas som sig bör i dessa situationer både hos polisen och i ett privat företag som behandlar uppgifter. I lagför-

slaget beaktas också behovet av s.k. förenlig behandling av personuppgifter i sådana fall där det kan bli nödvändigt att behandla personuppgifter inom tillämpningsområdet för två EU-rättsakter om dataskydd.

I det 1:a lagförslagets 4 kap. 4 § ges polisens tillståndsförvaltning större möjligheter än i nuläget när det gäller att lämna ut personuppgifter till sammanslutningar och näringsidkare genom elektronisk kommunikation. Med avseende på konsekvenserna för företag bör det noteras att enligt detaljmotiveringen till den föreslagna paragrafen ska de privata sammanslutningar och näringsidkare till vilka information får lämnas ut inte specificeras i paragrafen, utan mottagarna ska begränsas utifrån sina uppgifter, som fastställs annanstans i lagstiftningen. Med andra ord följer konsekvenserna för företag inte direkt av det 1:a lagförslaget, utan även de preciseras via den övriga lagstiftningen om de privata sammanslutningarnas och näringsidkarnas uppgifter.

Anpassningen till och iakttagandet av lagstiftningen medför affärskostnader för företag, men samtidigt också positiva effekter för affärsverksamheten. Största delen av dessa ekonomiska konsekvenser och konsekvenserna för konkurrensen föranleds dock av annan lagstiftning än genomförandebestämmelserna i dataskyddslagstiftningen eller det 1:a lagförslaget, bl.a. av passlagen och lagen om identitetskort eller skjutvapenlagen. Det kan vara fråga om engångskostnader, såsom de kostnader för ändring av informationssystem som orsakas i synnerhet av personuppgiftsbehandling för polisens behov och som behövs för att personuppgifter ska kunna lämnas ut från företagets informationssystem. Det att personuppgifter vid tillhandahållande av tjänster för myndigheter, vilket beaktas i det 1:a lagförslaget i propositionen, ska behandlas på ett behörigt sätt så att kraven i den nya dataskyddsförordningen beaktas till fullo med avseende på den personuppgiftsansvarige vid polisen medför dock i viss mån kostnadskonsekvenser även för företagen. I detta avseende ska det i synnerhet beaktas att ansiktsbilder och fingeravtryck har karaktären av känsliga personuppgifter, vilket ställer högre krav på informationssäkerheten i informationssystemen. Samtidigt gäller den nya dataskyddsförordningen i vilket fall som helst samtliga företag, vilket innebär att de krav som den ställer på behandlingen av personuppgifter ska beaktas även för tillhandahållandet av andra tjänster. De självständiga konsekvenserna av det 1:a lagförslaget bedöms således i egenskap av indirekta konsekvenser vara skäliga, medan de direkta konsekvenserna uppstår i och med iakttagandet av EU:s dataskyddsförordning. Samtidigt uppskattas det 1:a lagförslaget i kombination med tillämpningen av den allmänt tillämpliga nya dataskyddslagstiftningen ha en positiv effekt på företagens verksamhet. Tillförlitlig behandling av personuppgifter har potentiellt en förtroendehöjande effekt som ökar användningen av tjänsterna. Med tanke på att en övervägande del av de ekonomiska konsekvenserna för företag orsakas av annan lagstiftning om tillhandahållande av tjänster bedöms lagförslaget om personuppgiftsbehandling inom polisväsendet inte få några betydande personalkonsekvenser.

Konsekvenser för statsfinanserna

[I den fortsatta beredningen kompletteras propositionens förhållande till den tilläggsbudgetproposition som kompletterar budgeten för 2018, med vilken de obligatoriska kostnadskonsekvenser som följer av genomförandet av dataskyddslagstiftningen ska täckas till den del den befintliga finansieringen inte räcker till för att täcka dem.]

Konsekvenser för personalresurserna. EU-lagstiftningen om dataskydd kräver att varje personuppgiftsansvarig ska ha ett dataskyddsombud. Enligt det 1:a lagförslaget ska polisen ha tre personuppgiftsansvariga, nämligen skyddspolisen (skyddspolisens funktionella personregister), centralkriminalpolisen (penningtvättsregistret) och Polisstyrelsen (polisens övriga riksomfattande personregister). Vidare ska Polisstyrelsen ha en personuppgiftsansvarig för behandling av sådana passageraruppgifter som avses i det 2:a lagförslaget. Enligt PNR-direktivet

ska ett dataskyddsombud utnämnas för enheten för passagerarinformation. Ombudets uppgifter är något mer omfattande än de uppgifter som sköts av de dataskyddsombud som ska utnämnas med stöd av dataskyddsdirektivet. Dataskyddsombudet för enheten för passagerarinformation har redan utnämnts. Dataskyddsombudet kan med stöd av EU-lagstiftningen om dataskydd också bestå av ett gemensamt dataskyddsombud för flera personuppgiftsansvariga, om detta betraktas som ändamålsenligt. Skyddspolisen och Polisstyrelsen har sedan tidigare utnämnda dataskyddsombud, men vid centralkriminalpolisens central för utredning av penningtvätt finns för tillfället ingen tjänst för ett dataskyddsombud, varför en indirekt direkt konsekvens av det 1:a lagförslaget med avseende på personalresurser blir högst 1 årsverke. Det återstår att överväga om ett särskilt dataskyddsombud måste utnämnas för centralkriminalpolisen i dess egenskap av personuppgiftsansvarig för det register som förs av centralen för utredning av penningtvätt, eller om ett och samma dataskyddsombud kunde utnämnas också för centralkriminalpolisens övriga behandling av personuppgifter. Det 1:a lagförslaget i propositionen medför inga andra konsekvenser för personalresurserna, och propositionen kräver således till denna del ingen tilläggsfinansiering.

Det 2:a lagförslaget i propositionen får direkta konsekvenser för personalresurserna, och dessa specificeras nedan myndighetsvis. Konsekvenserna gäller polisen och dataombudsmannens byrå (nedan dataskyddsmyndigheten).

Informationssystemsprojekt och ändringar av informationssystem. Det 1:a och det 2:a lagförslaget i propositionen hänför sig i väsentlig grad till polisens informationssystemsprojekt. Direkta konsekvenser för informationssystemen får bl.a. de utvidgningar av personuppgiftsbehandlingen som föreslås i det 1:a lagförslagets 2 kap. Som exempel kan nämnas den föreslagna bestämmelsen om behandling av personuppgifter för ändamål som tjänar kriminalunderrättelseinhämtning, vilket i praktiken innebär att ett nytt register för kriminalunderrättelseinhämtning ska inrättas. Även bestämmelserna om utlämnande av uppgifter i 3 och 4 kap., bestämmelserna om utplåning i 5 kap. och bestämmelserna om den registrerades rättigheter i 6 kap. får direkta konsekvenser för informationssystemen. En del av dessa konsekvenser är emellertid ändringar som genomförs i redan befintliga informationssystem eller som kan genomföras med hjälp av projektfinansiering. De föreslagna bestämmelserna i det 1:a lagförslaget medför också indirekta konsekvenser för de övriga myndigheternas informationssystem, till vilka anslutningsgränssnitt ska byggas upp.

För reformen av polisens informationssystem har det s.k. Vitja-projektet tillsatts för perioden 1.10.2017–31.12.2020. Syftet är att verksamhetsstyrningssystemet Vitja ska ersätta dels, till tillämpliga delar, det nuvarande informationssystemet för polisärenden (Patja) i den omfattning som avses i 2 kap. 2 § i den gällande personuppgiftslagen för polisväsendet, dels informationssystemet för misstänkta (Epri). Polisstyrelsen fastställer varje år en finansieringsram för Vitja-projektet. Regleringslösningarna i lagförslaget anknyter direkt till Vitja-projektet. Nedan specificeras närmare vilka informationssystemsändringar som till alla delar ska genomföras inom ramen för Vitja-projektet och som således inte kräver tilläggsfinansiering ur statsbudgeten. Även i fråga om registret för kriminalunderrättelseinhämtning har det uppskattats att kostnaderna för inrättandet av registret till alla delar kan täckas med finansieringen för Vitja-projektet.

Det 2:a lagförslaget i propositionen är förknippat med ett informationssystemsprojekt genom vilket det nationella informationssystem som förutsätts i PNR-direktivet genomförs, inklusive tillhörande tekniska lösningar för mottagande av personuppgifter från lufttrafikföretagen. Utvecklingen av informationssystemet har till stor del finansierats ur fonden för inre säkerhet, och avsikten är att de resterande kostnaderna ska täckas med projektfinansiering. Utvecklingsarbetet och uppfyllandet av kraven enligt dataskyddsdirektivet i de system som ska utvecklas för behandling av passageraruppgifter kräver ingen tilläggsfinansiering ur statsbudgeten.

Systemen för behandling av passageraruppgifter uppskattas ändå orsaka årliga kostnader på sammanlagt 3–4 000 000 euro. Det handlar om kostnader för driften av informationssystemet och andra servicekostnader samt kostnader för småskalig utveckling. Utöver den finansiering som beviljats har det uppskattats att projektets genomförande kräver en tilläggsfinansiering på cirka 2,1 miljoner euro fram till år 2020. Tilläggsfinansiering ska sökas separat från fonden för inre säkerhet. [*Dessutom uppskattas genomförandet av projektet kräva en ökning av polisens omkostnader – kompletteras i samband med den fortsatta beredningen*]

Genomförandet av dataskyddsdirektivet och dataskyddsförordningen är till vissa delar förknippat med vissa direkta och indirekta informationssystemsändringar, som presenteras noggrannare nedan. En del av dessa ska inte genomföras i de befintliga systemen, och den befintliga finansieringen räcker inte till för att täcka alla obligatoriska ändringar. Till en viss del kan konsekvenserna täckas med den ovannämnda finansieringen av Vitja-projektet, som dock gäller enbart Polisstyrelsen som personuppgiftsansvarig. Till den del de obligatoriska informationssystemsändringarna enligt dataskyddslagstiftningen inte kan täckas med befintlig finansiering har inrikesministeriet för avsikt att bereda en tilläggsbudgetproposition som kompletterar budgeten för 2018. Tilläggsbudgetpropositionen och denna proposition ska överlämnas samtidigt. Åtminstone de informationssystemsändringar som måste göras vid centralen för utredning av penningtvätt kräver en tilläggsbudget. [*De kostnader som kräver en tilläggsbudget bedöms närmare under den fortsatta beredningen*.]

Skadestånd och administrativa påföljder. Påföljderna av överträdelser som gäller behandling av personuppgifter fastställs i enlighet med dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Det 1:a och det 2:a lagförslaget i denna proposition får till denna del inga självständiga konsekvenser för statsfinanserna. Eventuella skadestånd som påförs för överträdelser av lagstiftningen ska betalas i enlighet med skadeståndslagen. Regleringen har direkta effekter på statens utgifter. Det är dock omöjligt att förutspå och i detalj beräkna hur stora utgifter det handlar om per år.

Med stöd av det 2:a lagförslaget kan dessutom en administrativ påföljdsavgift påföras ett lufttrafikföretag i det fall att företaget försummar sin skyldighet att till polisen överföra de passageraruppgifter som förutsätts i lag. Påförandet av påföljdsavgifter med stöd av den nya lagen får konsekvenser för statsfinanserna, men de uppskattas inte bli betydande. Samtidigt orsakas Rättsregistercentralen en administrativ börda och skäliga kostnader för inkasseringen av avgifterna. I fråga om andra trafikföretag kan polisen på motsvarande sätt som i den gällande lagen förena en enskild begäran om utlämnande av uppgifter med vite. Eftersom det inte föreslås att denna bestämmelse ska ändras medför propositionen till denna del inga direkta konsekvenser för statsfinanserna.

De påföljdsavgifter som tas ut med stöd av det 2:a lagförslaget i propositionen intäktsförs i statsbudgeten [under moment 12.39.01 (Böter och inkomster från administrativa betalningspåföljder)]. Det är fråga om en ny administrativ påföljdsavgift, och det finns inga tidigare erfarenheter av den. Därför kan endast osäkra uppskattningar av det årliga beloppet av dessa inkomster presenteras. Gränsbevakningsväsendet har emellertid redan med stöd av den gällande lagstiftningen rätt att ta ut en påföljdsavgift av en transportör som bryter mot den kontrollskyldighet som föreskrivs i 173 § i utlänningslagen eller den skyldighet för lufttrafikföretag att lämna uppgifter som avses i 20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (uppgifter om passagerare inom flygtrafiken). Avgiften för brott mot 173 § i utlänningslagen är 3 000 euro för varje person som transporterats och avgiften för brott mot 20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet är 3 000 euro för varje sådan resa för vilken uppgifter om passagerare inte meddelats eller för vilken bristfälliga eller felaktiga uppgifter meddelats. Det sammanlagda antalet påföljdsavgifter som påförts varje år är som följer: 112 påföljdsavgifter år 2013, 163 påföljdsavgifter år 2014, 167 påföljdsavgifter

år 2015, 133 påföljdsavgifter år 2016 och 55 påföljdsavgifter år 2017 (antal påföljdsavgifter som inkommit till Rättsregistercentralen för verkställighet fram till 18.10.2017). Beloppet av de påföljdsavgifter som ska intäktsföras till staten har således varit knappt eller drygt 500 000 euro per år. Enligt 14 § i det 2:a lagförslaget i propositionen ska påföljdsavgiften för lufttrafikföretag vara högst 3 000 euro för varje sådan flygning för vilken passageraruppgifter inte har överförts eller för vilken uppenbart bristfälliga uppgifter överförts. Beloppet överensstämmer således med det maximibelopp som anges i lagen om gränsbevakningsväsendet. Utifrån de påföljdsavgifter som påförts av gränsbevakningsväsendet kan man grovt uppskatta ungefär vilken mängd påföljdsavgifter som är att vänta. Antalet påföljdsavgifter som påförs med stöd av det 2:a lagförslaget kan variera avsevärt, och detsamma gäller således de belopp som intäktsförs till staten. För lufttrafikföretagens del skiljer sig skyldighetens innehåll och det sätt på vilket uppgifterna ska överföras enligt det 2:a lagförslaget från den gällande lagstiftningen om gränsbevakningsväsendet, och det är därför omöjligt att presentera säkra kalkyler.

Andra konsekvenser för statens inkomster och utgifter. Propositionen har inga andra direkta konsekvenser vad gäller statens inkomster. Exempelvis avgifterna i tillståndsärenden grundar sig på annan lagstiftning. En mer detaljerad och högklassig dataskyddsreglering på EU-nivå kan emellertid bedömas få indirekta konsekvenser för statens inkomster. Målet med bestämmelserna i 2 kap. i det 1:a lagförslaget är att uppnå en teknikneutral reglering av personuppgiftsbehandlingen, så att det blir möjligt att i bredare skala utveckla och utnyttja digitala datanätstjänster t.ex. i tillståndsförvaltningsärenden. Redan i nuläget sker behandlingen av personuppgifter i tillståndsärenden delvis med hjälp av e-tjänster som används via det allmänna datanätet, så att t.ex. den sökande kan skriva under sin ansökan digitalt och lägga till en digital ansiktsbild som behandlats av ett fotograferingsföretag. Det att e-tjänster utnyttjas i allt högre grad i behandlingen av personuppgifter kan på lång sikt uppskattas ha en minskande effekt på behovet av personalresurser. På motsvarande sätt är ambitionen också att möjliggöra en teknikneutral reglering av personuppgiftsbehandlingen i anslutning till brottmål. På så sätt kan informationssystemen utvecklas så att det får en minskande effekt på polisens manuella arbete. På lång sikt kan en positiv effekt av regleringen vara att statens utgifter minskar.

4.2 Konsekvenser för samhällsekonomin och totalekonomiska konsekvenser

EU-lagstiftningen om dataskydd får omfattande ekonomiska konsekvenser för uppfyllandet av de skyldigheter som följer av lagstiftningen och som gäller alla myndigheter och företag. Dessa konsekvenser orsakas direkt av dataskyddsförordningen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. För myndigheterna orsakar genomförandet av skyldigheterna ändringsbehov i fråga om flera informationssystem, och de sammanlagda kostnaderna för dessa är betydande även totalekonomiskt sett. Vidare ska varje personuppgiftsansvarig utnämna ett dataskyddsombud. På lång sikt sporrar den nya dataskyddslagstiftningen ändå till att utveckla informationssystemen så att de blir säkrare och så att informationssäkerheten förbättras. Dessutom kan de mer detaljerade bestämmelserna om registerföring och tillsynen över registren och de nya administrativa påföljderna förväntas leda till att riskerna för dataskyddsförseelser och kränkningar av informationssäkerheten minskar. Detta kan på lång sikt bedömas få positiva totalekonomiska effekter. Samtidigt finns det många osäkerhetsfaktorer när det gäller bedömningen och utfallet av de ekonomiska risker som är förknippade med behandlingen av personuppgifter, och det är omöjligt att exakt bedöma vilken effekt dessa kommer att ha. Vidare bygger regleringens konsekvenser på EU-lagstiftningen om dataskydd och dess genomförandebestämmelser samt på tillämpningen av bestämmelserna om personuppgiftsbehandling inom polisväsendet som helhet, vilket gör det svårare att bedöma de totalekonomiska konsekvenserna. Det 1:a lagförslaget har inga samhällsekonomiska eller totalekonomiska konsekvenser som är oberoende av EU-lagstiftningen.

4.3 Konsekvenser för myndigheterna

De bestämmelser i det 1:a lagförslaget som avviker från den gällande lagen får konsekvenser för olika myndigheter. Konsekvenserna bygger delvis indirekt på kraven i EU:s dataskyddsförordning och dataskyddsdirektivet och delvis på nationella regleringslösningar. Det 2:a lagförslaget får konsekvenser som orsakas direkt av genomförandet av PNR-direktivet.

Europeiska kommissionen har utfört en konsekvensbedömning på EU-nivå i fråga om EU-lagstiftningen om dataskydd (SEC(2012) 72 final). Kommissionens konsekvensbedömning omfattar genomförandet av såväl personuppgiftsdirektivet från år 1995 som dataskyddsrambeslutet. Både den personuppgiftslag som genomför direktivet från år 1995 och genomförandebestämmelserna för dataskyddsrambeslutet gäller polisen i Finland. Det faktum att medlemsstaterna har genomfört, tolkat och tillämpat direktivet från år 1995 på olika sätt har också försvårat samarbetet mellan myndigheterna. Problemet accentueras av den snabba tekniska utvecklingen och av att myndighetstjänsterna i allt högre grad överförs till det allmänna datanätet. Enligt Europeiska kommissionens bedömning har det fragmenterade genomförandet dock haft mindre konsekvenser för myndigheterna än för företagen, eftersom myndighetstjänster mest erbjuds personer som bor inom medlemsstatens gränser. Bestämmelserna i dataskyddsförordningen ger myndigheterna mer rörelseutrymme. Det är viktigt att dataskyddsnivån är hög både inom den privata sektorn och vid myndigheterna när det gäller brottsbekämpande myndigheters behov att i vissa situationer, för att de ska kunna sköta sina uppgifter, överlämna personuppgifter till privata företag.

De huvudsakliga problemen som kommissionen lyfter fram i fråga om dataskyddsrambeslutet hänför sig till rättsaktens begränsade tillämpningsområde och andra luckor i regleringen. Enligt kommissionens bedömning konkretiseras problemen i och med att det internationella samarbetet inom och över EU:s gränser ökar. Det finns också statistik som stöder denna bedömning. Bestämmelserna har också ansetts vara splittrade, med tanke på det oenhetliga genomförandet av dataskyddsrambeslutet. I dataskyddsdirektivet, som ersätter rambeslutet, har målsättningen varit att förenhetliga regleringen så att tillämpningsområdet utvidgas till att gälla all personuppgiftsbehandling i anslutning till brottmål, oavsett om det är fråga om gränsöverskridande överföringar av personuppgifter eller uppgiftsbehandling på nationell nivå. Kommissionen har haft som ambition att säkerställa att individens rättigheter garanteras fullt ut och att samtidigt skapa ett bättre förtroende för och underlätta polissamarbetet. Avsikten har också varit att genom det nya direktivet säkerställa att enhetliga och konsekventa principer tillämpas på all behandling av personuppgifter. Samma krav ska beaktas även vid internationella överföringar av personuppgifter. Målsättningarna med EU-lagstiftningen om dataskydd ska i huvudsak beaktas i det lagförslag som gäller behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I det 1:a lagförslaget, som kompletterar lagen om genomförande av direktivet och den allmänna dataskyddsförordningen, har den nya regleringen beaktats i fråga om såväl dataskyddsförordningen som dataskyddsdirektivet.

När det gäller behandling av personuppgifter i brottmål är den största ändringen i förhållande till den gällande lagstiftningen att de personuppgiftsansvariga vid EU:s polismyndigheter jämställs med de personuppgiftsansvariga vid polisen i Finland. Samarbetet inom EU går även med stöd av den nya lagstiftningen främst ut på att förebygga, utreda och avslöja brott. Samtidigt är syftet med lagförslaget att skapa en så enhetlig nationell reglering som möjligt oberoende av om behandlingen av personuppgifter i polisens verksamhet hör till dataskyddsförordningens eller dataskyddsdirektivets tillämpningsområde. Med tanke på att det är fråga om två olika rättsakter och eftersom medlemsstaterna definierar ett brottmål delvis på olika sätt finns det dock en risk för att medlemsstaternas genomförandelagstiftning alltjämt till vissa delar förblir oenhetlig trots den nya regleringen. Målsättningen med det 1:a lagförslaget är ändå att detta inte ska störa medlemsstaternas polissamarbete till den del det är fråga om utlämnande

av personuppgifter. Till denna del föreslås inte heller några större ändringar i bestämmelserna. I lagförslaget har behovet av enhetligare bestämmelser på EU-nivå när det gäller överföring av personuppgifter till tredjeländer och internationella organisationer beaktats till kompletterande delar. Även till denna del har regleringen skärpts i förhållande till den gällande bestämmelserna. Framför allt betonas det tydligare än tidigare att dataskyddsnivån i ett tredjeland inte automatiskt kan anses vara tillräckligt hög, utan dataskyddsnivån ska bedömas separat och den kan också förändras. Det ska finnas juridiska garantier på att dataskyddsnivån är tillräckligt hög. Målsättningen med den nya striktare regleringen är att säkerställa skyddet av den registrerades rättigheter även i sådana fall där personuppgifter överförs över gränserna.

Genom bestämmelserna om förenlig behandling av personuppgifter i det 1:a lagförslaget, som i viss mån utvidgar de behandlingsändamål som ska betraktas som förenlig behandling av personuppgifter, har man eftersträvat att säkerställa polisens verksamhetsförutsättningar dels i situationer där det enligt motiveringen till direktivet är svårt att på förhand avgöra om det är fråga om att upprätthålla den allmänna ordningen och säkerheten eller att förebygga, avslöja eller utreda ett brott, dels i situationer där det är nödvändigt att kontrollera personuppgifter i flera olika personregister för att effektivt kunna förebygga, avslöja och utreda ett brott. Som förenlig behandling av personuppgifter betraktas också sådana fall där uppgifter som ursprungligen samlats in och lagrats för behandlingsändamål som är förenliga med dataskyddsdirektivet används för att utreda villkoren för beviljande av tillstånd eller för ett tillstånds giltighet. Bestämmelserna innebär en inskränkning av den registrerades integritetsskydd. I de föreslagna bestämmelserna i fråga har strävan dock varit att beakta de i dataskyddsdirektivet angivna skärpta och harmoniserade kraven på att avvikelser från ändamålsbegränsningen av personuppgiftsbehandlingen ska begränsas strikt till sådan behandling av personuppgifter som är förenlig med det ursprungliga ändamålet med behandlingen av uppgifterna. Lagförslaget anses också garantera att den registrerades rättigheter säkerställs effektivare än tidigare i polisens arbete. Till detta bidrar förutom den enhetliga EU-regleringen om ändamålsbegränsning, den registrerades rätt att bli informerad och den registrerades direkta eller indirekta rätt till insyn särskilt bestämmelserna om tillsynen över registerföringen. Den registrerades rättigheter tryggas också av dataskyddsmyndigheternas enhetliga och omfattande befogenheter, som delvis är gränsöverskridande, och av att lagstiftningen om behandling av personuppgifter hör till EU-domstolens behörighet.

Majoriteten av konsekvenserna av det 1:a lagförslaget rör behandlingen av personuppgifter vid polisenheterna. För de övriga myndigheternas del gäller konsekvenserna av lagförslaget främst sådana bestämmelser som gäller utlämnande av personuppgifter till andra myndigheter. De största konsekvenserna för myndigheterna hänför sig till registerföringen. När det gäller sådan personuppgiftsbehandling som utförs av polisen finns de mest betydande ändringarna jämfört med nuläget i 2, 4 och 5 kap. i det 1:a lagförslaget och i det 2:a lagförslaget.

Förslaget att ersätta den registerbaserade regleringen med en reglering som utgår från behandlingsändamålen orsakar en administrativ börda för både den personuppgiftsansvarige och för de polisenheter som tillämpar lagen. Bördan orsakas i synnerhet av behovet av anvisningar och utbildning. I 4 kap. i det 1:a lagförslaget föreskrivs det om utlämnande av personuppgifter till andra myndigheter och till informationssystem på EU-nivå. I fråga om dessa bestämmelser föreslås ändringar i den gällande regleringstekniken och till vissa delar även utvidgningar i rättigheterna att lämna ut uppgifter. Dessa ändringar i kombination med regleringstekniken i 2 kap. har betydelse också för utlämnandet av personuppgifter mellan EU-medlemsstaterna. Ändringarna orsakar en viss administrativ börda i synnerhet i form av anvisningar och utbildning. Lagförslagets 4 kap. innehåller också bestämmelser om utlämnande av personuppgifter till tredjeländer och internationella organisationer. Bestämmelserna kompletterar lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Inga betydande innehållsmässiga ändringar i förhållande till den gällande lagen föreslås i dessa bestämmelser.

Bestämmelserna i 4 kap., som är helt nya, orsakar en viss administrativ börda för polisen. Dessa bestämmelser uppskattas i viss mån leda till att utlämnandet av personuppgifter ökar, trots att utlämnande av personuppgifter alltid utgör enskilda fall där personuppgifter måste lämnas ut till en annan myndighet för att förebygga, avslöja eller utreda ett brott, och trots att varje enskilt fall är beroende av det aktuella ärendets natur. Jämfört med den gällande lagen innehåller förslaget emellertid bara en helt ny situation där personuppgifter får lämnas ut, nämligen när uppgifter om tillstånds giltighet lämnas ut till privata sammanslutningar och näringsidkare genom elektronisk kommunikation, varför de totala konsekvenserna kan uppskattas bli tämligen obetydliga. Samtidigt bedöms de föreslagna bestämmelserna effektivisera samarbetet mellan myndigheterna.

I bestämmelserna om utplåning av personuppgifter föreslås betydande ändringar. Ändringarna medför ett behov av anvisningar för de experter som ansvarar för informationssystemen, vilket innebär att de nya bestämmelserna om utplåning i 5 kap. medför en viss administrativ börda för den personuppgiftsansvarige.

Polisstyrelsen. De mest betydande konsekvenserna av EU-lagstiftningen om dataskydd och dess genomförandebestämmelser samt det 1:a lagförslaget i propositionen rör Polisstyrelsen som, med undantag av de register som förs av centralen för utredning av penningtvätt vid centralkriminalpolisen och skyddspolisen, ansvarar för registerföringen i anslutning till polisens riksomfattande informationssystem. Övergången från registerbaserad reglering till en reglering som baserar sig på ändamålen med personuppgiftsbehandlingen påverkar i regel inte ansvarsfördelningen i fråga om de befintliga informationssystemen. Polisstyrelsen ska också ansvara för registerföringen av registret för kriminalunderrättelseinhämtning, som ersätter registret för misstänkta. De gällande bestämmelserna om registerföringen innehåller redan i huvudsak sådana krav som motsvarar den nya dataskyddsregleringen. De nya bestämmelserna är dock mer detaljerade och striktare.

Revideringen av EU-lagstiftningen om dataskydd medför en betydande ökning av den administrativa bördan för den personuppgiftsansvarige. En bidragande faktor kan vara att de registrerade utnyttjar sina rättigheter mer aktivt än tidigare i och med att medvetenheten om dataskyddsregleringen ökar och tillsynsmyndigheterna får större befogenheter. Det är dock omöjligt att i detalj bedöma i vilken mån de registrerade kommer att utnyttja sina rättigheter. Kostnadskonsekvenserna hänför sig huvudsakligen till skötseln av dataskyddsombudens uppgifter, men eventuellt också till företrädandet av den personuppgiftsansvarige i förvaltningsrättsliga och straffrättsliga förfaranden. Den registrerade har fått större rättigheter även på EU-nivå genom att det i lagstiftningen föreskrivs uttryckligen om användningen av rättsmedel i gränsöverskridande situationer och genom att dataskyddsmyndigheternas befogenheter utvidgas till att omfatta hela EU. Med tanke på detta måste de personuppgiftsansvariga, eventuellt genom en resursökning, förbereda sig på att dessa rättigheter kommer att utnyttjas. Den personuppgiftsansvarige måste också förbereda sig på ett eventuellt effektivare inriktat skadeståndsansvar. Å ena sidan kan resursbehovet länkas ihop med skötseln av andra uppgifter, vilket minskar den administrativa bördan. Å andra sidan ökar den administrativa bördan något i och med skyldigheten att på ett nytt sätt informera de registrerade om behandlingen av personuppgifter samt skyldigheten att informera dem om kränkningar av informationssäkerheten. Vissa skyldigheter ingår emellertid redan i den gällande lagstiftningen, och den totala konsekvensen kan således till denna del anses vara skälig.

Mer betydande konsekvenser uppskattas följa av de mer detaljerade kraven på registerföring och tillsyn över registren. Den personuppgiftsansvarige ska enligt de nya EU-bestämmelserna

om dataskydd uttryckligen påvisa att den personuppgiftsansvarige iakttar lagstiftningen om personuppgiftsbehandling inom polisväsendet. Den personuppgiftsansvarige har enligt den nya regleringen också mer detaljerade skyldigheter att dokumentera personuppgiftsbehandlingen, inklusive information om vilken typ av personuppgifter som lämnats ut och till vilka mottagare. Den personuppgiftsansvarige ska göra en bedömning av dataskyddskonsekvenserna när nya åtgärder för personuppgiftsbehandling vidtas, vilket inte ingår som en uttrycklig skyldighet i de gällande bestämmelserna. Enligt de nya bestämmelserna är det dessutom, liksom även i den gällande lagstiftningen, obligatoriskt att höra dataskyddsmyndigheten i vissa situationer, men också dessa bestämmelser är mer detaljerade än tidigare. Förutom att den registrerade ska informeras om kränkningar av informationssäkerheten är den personuppgiftsansvarige också skyldig att underrätta tillsynsmyndigheten om sådana situationer. Den administrativa börda som följer av dessa skyldigheter kan anses vara betydande.

Den personuppgiftsansvarige orsakas en administrativ börda också i det avseendet att personuppgiftsbiträdena ska förbinda sig till de nya kraven genom nya avtal. I EU-lagstiftningen om dataskydd beaktas förhållandet och de inbördes skyldigheterna mellan den personuppgiftsansvarige och personuppgiftsbiträdena i större detalj än tidigare. Utöver detta ska den personuppgiftsansvarige använda resurser till att utveckla personalens kompetens. Det uppstår oundvikligen ett behov av nya typer av anvisningar och utbildning i och med de mer detaljerade och striktare allmänna kraven på personuppgiftsbehandling, skillnaderna mellan tillämpningsområdena för EU:s dataskyddsförordning och dataskyddsdirektivet samt ändringarna i den nationella regleringen av personuppgiftsbehandling inom polisväsendet, såsom övergången till en reglering som utgår från behandlingsändamålen. De nationella regleringslösningarna och totalreformen av dataskyddsregleringen innebär i praktiken att hela personalen ska introduceras i den nya regleringen. Den personuppgiftsansvarige och de som utövar polisens interna laglighetskontroll ska också följa upp att kraven iakttas, vilket orsakar en administrativ börda.

Myndigheterna har till en del redan förberett sig på de krav som den nya dataskyddsregleringen ställer. Den administrativa börda som orsakas av de nya kraven blir lättare i och med att genomförandet fördelas över en längre tidsperiod. Polisstyrelsen har dessutom redan sedan tidigare ett utnämnt dataskyddsombud. Innehållet i dataskyddsombudets uppgifter har redan på förhand preciserats så att de i praktiken uppfyller kraven enligt dataskyddslagstiftningen. Polisstyrelsen ansvarar som enda personuppgiftsansvarig vid polisen för registerföringen i anslutning till det informationssystem som förs för skötseln av de uppgifter som anges i 1 kap. 1 § i polislagen och som hör till dataskyddsförordningens tillämpningsområde, vilket innebär att högre krav ställs på dataskyddsombudet. Samma personer ska vara dataskyddsombud även i fråga om sådan personuppgiftsbehandling som hör till dataskyddsdirektivets tillämpningsområde.

Centralkriminalpolisen. Centralkriminalpolisen är personuppgiftsansvarig för det penningtvättsregister som förs av centralen för utredning av penningtvätt. Centralkriminalpolisen orsakas motsvarande konsekvenser till den del det är fråga om den administrativa börda som följer av den personuppgiftsansvariges ansvar. För det enskilda registret blir den administrativa bördan och kostnadskonsekvenserna emellertid avsevärt mindre. Centralen för utredning av penningtvätt har dock tills vidare inget utnämnt dataskyddsombud och behöver således tilläggsresurser motsvarande uppskattningsvis ett årsverke för den uppgift som bygger på dataskyddslagstiftningen, i det fall att ett eget dataskyddsombud utnämns för centralen. De krav som ställs på dataskyddsombudet grundar sig på en i dataskyddsdirektivet angiven nivå, och skötseln av dataskyddsombudets uppgifter och kontakten till dataskyddsmyndigheten orsakar en administrativ börda för centralen för utredning av penningtvätt.

Centralkriminalpolisen, i dess egenskap av en riksomfattande enhet inom polisen, dess personal och även personalen vid centralen för utredning av penningtvätt ansvarar för egen del för

att de nya krav som ställs på behandlingen av personuppgifter iakttas. När det gäller personuppgiftsbehandling får det 1:a lagförslaget konsekvenser för personalen i enlighet med lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, beroende på för vilket ändamål personuppgifter behandlas. Den egna behandlingen av personuppgifter vid centralkriminalpolisen och centralen för utredning av penningtvätt hör i regel till tillämpningsområdet för EU:s dataskyddsdirektiv och dess genomförandelagstiftning, vilket, i jämförelse med polisinrättningarna, i viss mån minskar den börda som orsakas personalen. Det krävs emellertid tid och inskolning bl.a. genom utbildning och anvisningar för att personalen ska tillägna sig de nya kraven, som är mer detaljerade och striktare. Dessutom är det viktigt att också dessa polisenheter ger akt på dels eventuella situationer som innefattar sådan personuppgiftsbehandling som hör till dataskyddsförordningens tillämpningsområde, dels vid behov situationer där behandlingsändamålet för personuppgifter som samlats in för ett sådant ändamål som hör till dataskyddsförordningens tillämpningsområde förändras. I fråga om personalen framhävs också de närmaste chefernas ansvar för övervakningen av användningen av informationssystemen och för inskolningen i denna övervakning.

Skyddspolisen. Skyddspolisen ansvarar i framtiden på samma sätt som i nuläget för registerföringen i anslutning till skyddspolisens funktionella informationssystem. Dessutom är skyddspolisen personuppgiftsansvarig för det register över säkerhetsutredningar som avses i säkerhetsutredningslagen (726/2014) och som varit i funktion sedan hösten 2017. Behandling av personuppgifter vid skyddspolisen hör inte till tillämpningsområdet för EU-lagstiftningen om dataskydd, men i det 1:a lagförslaget i propositionen föreslås att lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska tillämpas på skyddspolisens personuppgiftsbehandling, med vissa begränsningar som framgår av lagförslaget. Syftet med reformen är dock inte att i någon betydande grad ändra behandlingen av personuppgifter vid skyddspolisen.

Skyddspolisen orsakas motsvarande konsekvenser till den del det är fråga om den administrativa börda som följer av den personuppgiftsansvariges ansvar. Skyddspolisen har ett utnämnt dataskyddsombud för skyddspolisens funktionella informationssystem, så till denna del förorsakar den nya dataskyddslagstiftningen inga behov av tilläggsresurser. Dataskyddsombudets uppgifter är dock precis som de uppgifter som sköts av motsvarande personer vid de övriga polisenheterna mer detaljerade än tidigare, och oavhängigheten i förhållande till den operativa verksamheten framhävs tydligare än tidigare. För registret över säkerhetsutredningar ska ett separat dataskyddsombud utnämnas. Detta i kombination med den administrativa börda som orsakas det nya registret ger upphov till ett tilläggsresursbehov på cirka ett årsverke. De krav som ställs på dataskyddsombudet motsvarar de krav som fastställs i dataskyddsdirektivet. Skyddspolisen orsakas också motsvarande konsekvenser som de övriga polisenheterna när det gäller att utbilda personalen om de nya bestämmelserna och kraven och att övervaka att de iakttas.

Polisinrättningarna. Det 1:a lagförslaget får konsekvenser för polisinrättningarna och deras personal i enlighet med vad som föreskrivs i dataskyddsförordningen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, beroende på för vilket ändamål personuppgifter behandlas. Konsekvenserna av EU-lagstiftningen om dataskydd blir mindre för polisinrättningarna än för de personuppgiftsansvariga. EU-lagstiftningen om dataskydd medför också mer detaljerade bestämmelser och ett större ansvar för behandlingen av personuppgifter i polisens vardagliga arbete, vilket framhäver betydelsen av utbildning och övervakning i fråga om användningen av registren, inklusive de närmaste chefernas övervakningsansvar. De poliser som behandlar personuppgifter orsakas också vissa utmaningar i och med att personuppgiftslagen för polisväsendet inte längre kompletteras av den gällande allmänt tillämpliga personuppgiftslagen utan av tre allmänt tillämpliga författningar; EU:s dataskyddsförordning, som tillämpas på tillståndsärenden och relaterade tillsyn-

särenden, dataskyddslagen och en särskild lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Det innebär ett annat regelverk än tidigare, och dessutom är tillämpningsområdena för dessa författningar förknippade med gränsdragningssituationer. De olika situationerna när det gäller att tillämpa dessa författningar konkretiseras tydligast i den personuppgiftsbehandling som utförs vid polisinrättningarna.

Dataombudsmannens byrå/dataskyddsmyndigheten. Dataombudsmannens byrå ska i enlighet med det förslag till dataskyddslag som beretts av justitieministeriet ersättas med en ny dataskyddsmyndighet. När det gäller dataskyddsmyndighetens verksamhet medför lagförslagen i propositionen ekonomiska konsekvenser främst i form av ett personalresursbehov. Den nationella tillsynsmyndigheten ska med stöd av lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, dataskyddsförordningen och dataskyddslagen bl.a. kontrollera att uppgiftsbehandlingen är lagenlig, om den registrerades rätt till insyn har inskränkts, samt utföra undersökningar, verifieringar och granskningar. Dessa skyldigheter konkretiseras i och med tillämpningen av det 1:a lagförslaget i propositionen. De föreslagna ändringarna av regleringstekniken i det 1:a lagförslaget, såsom att personuppgiftsbehandlingen ska utgå från behandlingsändamålen, och ändringarna i behandlingen av personuppgifter som hänför sig till kriminalunderrättelseinhämtning kommer efter att lagen trätt i kraft att kräva ovannämnda övervakningsåtgärder. Sådan behandling av personuppgifter enligt det föreslagna 2 kap. 7 § 2 mom. som utförs för att klarlägga om uppgifterna behövs innebär en ökad rätt att inskränka integritetsskyddet och därmed ett ökat behov av övervakning och styrning. Det 2:a lagförslaget i propositionen får även direkta konsekvenser för dataskyddsmyndighetens uppgifter. Det 2:a lagförslaget medför en helt ny övervakningsuppgift med avseende på tillgodoseendet av den registrerades indirekta rätt till insyn till den del det är fråga om behandling av passageraruppgifter. Tilläggsbehovet av personalresurser blir 1,5 årsverken med betoning särskilt på tiden efter lagens ikraftträdande. I detta skede är det dock bara möjligt att göra en riktgivande bedömning av behovet av personalresurser.

Övriga myndigheter. Bestämmelserna i det föreslagna 4 kap., där regleringstekniken ändras i förhållande till den gällande lagen, orsakar i viss mån en större administrativ börda förutom för polisen även för de övriga myndigheterna. Det är dock omöjligt att göra en exakt bedömning av kostnadskonsekvenserna och de konsekvenser som medför en administrativ börda. Till den del det är fråga om utlämnande av personuppgifter till brottsbekämpande myndigheter och andra myndigheter som avses i dataskyddsdirektivet får uppgifter huvudsakligen utlämnas i samma situationer som tidigare trots att regleringstekniken ändras. Uppgifter kan även på samma sätt som nu utlämnas som en datamängd eller via en teknisk anslutning. Den administrativa börda som orsakas av tillämpningen av de föreslagna nya bestämmelserna, liksom av tillämpningen av de gällande bestämmelserna om utlämnande av personuppgifter, uppskattas således bli tämligen obetydlig. EU-lagstiftningen om dataskydd medför till denna del inte heller några betydande ändringar i fråga om utlämnande av personuppgifter när det gäller brottmål. När det är fråga om utlämnande av personuppgifter för ett förenligt ändamål får uppgifter utlämnas endast i nödvändiga fall när det nya ändamålet med personuppgiftsbehandlingen enligt strikta kriterier är förenligt med det ursprungliga behandlingsändamålet. Eftersom personuppgifter inte lämnas ut automatiskt i alla situationer kommer det i praktiken att uppstå rätt få situationer där denna bestämmelse tillämpas.

Bestämmelserna i det föreslagna 4 kapitlet avviker inte heller till sitt innehåll i betydande grad från den gällande lagen till den del det är fråga om utlämnande av personuppgifter till andra myndigheter än de myndigheter som avses i dataskyddsdirektivet. Det föreslagna 4 kap. möjliggör på samma sätt som i nuläget även i dessa situationer att personuppgifter under vissa förutsättningar kan utlämnas som en datamängd eller via en teknisk anslutning. Det föreslås emellertid att situationerna för utlämnande av uppgifter i flera avseenden ska utvidgas i förhållande till den gällande lagen. Detta leder till kostnadskonsekvenser främst för den myndighet

som tar emot personuppgifter i synnerhet i det fall att utlämnandet kräver att nya anslutningar öppnas eller förfrågningsgränssnitt byggs upp. Det har inte varit möjligt att under beredningen uppskatta exakt vilka konsekvenser de föreslagna utvidgningarna kommer att få. I dessa situationer medför det dessutom kostnadskonsekvenser och en administrativ börda när kraven i dataskyddslagstiftningen iakttas, i synnerhet när det gäller skyddet av personuppgifter. En del av dessa konsekvenser rör även polisen på det sätt som beskrivs ovan.

Den föreslagna 7 kap. 9 §, genom vilken skyddspolisen ges rätt att uppdatera sina egna informationssystem genom att jämföra dem med andra myndigheters personregister, har konsekvenser för de myndigheter ur vilkas system skyddspolisen hämtar uppdaterade personuppgifter till sina egna informationssystem. Skyddspolisen ska för det första ha rätt att få uppgifterna avgiftsfritt. Det kan medföra kostnader och extra arbete för den personuppgiftsansvarige att hämta uppgifter ur informationssystem för granskning och eventuellt kombinera dem. Detta ska emellertid om det är möjligt beaktas när uppgifter ur ett material begärs och när sådana begäranden avgränsas. I praktiken orsakar en begäran om uppgifter i viss mån en administrativ börda för mottagaren av begäran. Vidare ska skyddspolisen beakta den konsekvensbedömning som avses i 20 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. En skriftlig konsekvensbedömning av granskningen av jämförelseuppgifter ska upprättas för dataskyddsmyndigheten, som efter eget omdöme kan vidta åtgärder. Dessa åtgärder kan enligt den föreslagna lagen t.ex. gå ut på att förbjuda eller avbryta behandlingen av personuppgifter. Om det planeras att förfarandet ska upprepas med samma innehåll ska den skriftliga konsekvensbedömningen upprättas endast en gång. Den administrativa börda som orsakas dataombudsmannens byrå (senare dataskyddsmyndigheten) uppskattas således till denna del förbli skälig.

Brottsbekämpande myndigheter i EU-medlemsstater. Lagförslaget innehåller uttryckliga bestämmelser om utlämnande av personuppgifter till informationssystem på EU-nivå. Bestämmelserna ger akt på de krav som orsakas av den EU-lagstiftning som ska tillämpas på dessa informationssystem, inklusive den teknik som ska användas för utlämnande av personuppgifter. Genom det 1:a lagförslaget i propositionen genomförs på samma sätt som i den gällande lagen även Prümfördraget och Prümrådsbeslutet. Till den del EU-lagstiftningen har ändrats antas de justerade bestämmelserna få skäliga kostnadskonsekvenser för den behandling av personuppgifter som utförs av polisen. Detta gäller i synnerhet genomförandet av Europolförordningen, vars konsekvenser emellertid till största delen gör sig gällande via en särskild genomförandelag. Det föreslås dock att bestämmelserna om genomförandet av EU-lagstiftningen ska ändras till sina tekniska delar. Eftersom EU-regleringen i fråga om personuppgiftsbehandling innehållsmässigt har genomförts redan i den gällande personuppgiftslagen för polisväsendet förblir konsekvenserna av det 1:a lagförslaget till denna del ringa.

Myndigheter i tredjeländer. Den gällande lagen innehåller bestämmelser om utlämnande av personuppgifter till tredjeländer och internationella organisationer, och dessa bestämmelser motsvarar huvudsakligen lagförslaget. Det föreslås dock att sådana bestämmelser som överlappar med den allmänt tillämpliga lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska strykas. Den justerade språkdräkten orsakar inga behov av att ändra polisens praxis, och de bedöms således inte få betydande konsekvenser för personuppgiftsbehandlingen i tredjeländer eller Interpol. Den administrativa bördan orsakas i detta avseende främst polisen, med tanke på de striktare kraven på när det är tillåtet att utlämna personuppgifter och ansvaret för att skydda utlämnade personuppgifter på behörigt sätt oavsett hur de utlämnas. Den personuppgiftsansvariges ansvar gäller också utlämnande av personuppgifter till myndigheter i tredjeländer och Interpol.

Gränsöverskridande utbyte av uppgifter. När det gäller genomförandet av EU:s dataskyddsdirektiv, av vilket det 1:a lagförslaget utgör en del, har de mest betydande ekonomiska konse-

kvenserna uppskattats röra situationer där personuppgifter utlämnas över gränserna. De föreslagna bestämmelserna i kap. 4 medför en administrativ börda och kostnadskonsekvenser i synnerhet av den orsaken att de allmänt tillämpliga kraven i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska beaktas till fullo även när personuppgifter lämnas ut till tredjeländer eller Interpol. Polismyndigheterna i EU-medlemsstaterna ska jämställas med finländska polisenheter till den del det är fråga om utlämnande av personuppgifter. Dataskyddskraven är i jämförelse med det gällande dataskyddsrambeslutet avsevärt mer detaljerade i dataskyddsdirektivet, som genomförs genom den ovannämnda lagen. Iakttagandet av dessa krav medför en administrativ börda och i viss mån kostnadskonsekvenser för den personuppgiftsansvarige, i synnerhet när det är fråga om att begränsa behandlingen av personuppgifter eller rätta och utplåna personuppgifter samt att vidarebefordra och behandla personuppgifter som mottagits från en annan EU-medlemsstat. Den personuppgiftsansvarige ansvarar också för att personuppgifterna skyddas på behörigt sätt oberoende av på vilket sätt de lämnas ut. Vid utlämnande av personuppgifter mellan EU-medlemsstaternas polisenheter används emellertid sådana vedertagna kanaler för utlämnande av uppgifter som används redan i nuläget. I dessa har kraven på inbyggt dataskydd och dataskydd som standard i huvudsak beaktats. Dataskyddslagstiftningen får också betydande konsekvenser för brottsbekämpande myndigheter i tredjeländer när det gäller utbytet av uppgifter, med beaktande av att kraven på garanterat tillräckligt dataskydd har ändrats. Detta anses i praktiken bli relevant i synnerhet i sådana situationer där dataskyddsnivån inte anses vara tillräckligt hög med stöd av antingen Europeiska kommissionens beslut om nivån på dataskyddet eller ett bilateralt eller multilateralt avtal, varvid de nationella myndigheterna själva blir tvungna att förvissa sig om dataskyddsnivån. Med beaktande av att den förenhetligade EU-lagstiftningen ska tillämpas också på nationell behandling av personuppgifter är syftet med de föreslagna nya bestämmelserna samtidigt att öka förtroendet för att personuppgifter behandlas på behörigt sätt. De konsekvenser som dataskyddslagstiftningen och det 1:a lagförslaget i propositionen får med avseende på gränsöverskridande utbyte av uppgifter kan som helhet anses vara betydande.

Konsekvenser för informationssystemen. EU-lagstiftningen om dataskydd har direkta och indirekta konsekvenser för de nationella informationssystemen. Konsekvenserna konkretiseras i praktiken via kompletterande bestämmelser om enskilda myndigheter, såsom det 1:a lagförslaget i denna proposition. Kostnadskonsekvenserna av de nya kraven enligt dataskyddslagstiftningen eller av motsvarande krav enligt den tidigare lagstiftningen kan som helhet bli betydande till den del det är fråga om obligatoriska skyldigheter som tidigare inte har fullgjorts i informationssystemen. Kostnaderna varierar dessutom mellan de olika personuppgiftsansvariga, som för polisens del består av centralkriminalpolisen (penningtvättsregistret), skyddspolisen (skyddspolisens funktionella informationssystem) och Polisstyrelsen (polisens övriga riksomfattande personregister). Nedan redogörs för konsekvenserna per personuppgiftsansvarig beroende på vilken av EU-rättsakterna som ska tillämpas på dem, och dessutom bedöms vilka konsekvenser sådana nationella regleringslösningar som inte direkt föranleds av kraven i dataskyddsdirektivet får för informationssystemen.

Konsekvenserna har bedömts med avseende på de mest omfattande systemen som används på riksnivå. I nuläget bedöms reformen av dataskyddslagstiftningen emellertid sannolikt få konsekvenser för så gott som alla 70 system som polisen ansvarar för, eller åtminstone för verksamhetssätten och anvisningarna i anslutning till hanteringen av dessa system och de register som de innehåller. En del av kraven kan vara mycket svåra eller tekniskt sett rentav omöjliga att uppfylla till fullo, och ändringarna kan också leda till betydande kostnader. Polisstyrelsen uppskattar beroende på tolkningarna de totala kostnadskonsekvenserna av informationssystemsändringarna till minst flera hundratusen (minst 320 000 euro) och högst flera miljoner euro, rentav cirka tio miljoner euro.

Dataskyddsdirektivet

Direkta och indirekta kostnadskonsekvenser orsakas i synnerhet av de krav i dataskyddsdirektivet som går ut på att separera olika personkategorier från varandra i informationssystemen, om möjligt lagra personuppgifter som baserar sig på en personlig bedömning separat från verifierade personuppgifter, markera begränsningar av behandling av personuppgifter (på begäran av den registrerade eller någon annan myndighet eller en myndighet i en annan medlemsstat), granska loggar och i synnerhet fastställa motivering för olika åtgärder även utifrån utlämnande av uppgifter (sju års övergångsperiod), iaktta preciserade krav på informationssäkerhet, utvidga användningen av pseudonymisering och utvidga skyldigheten att utplåna uppgifter så att den eventuellt omfattar även säkerhetskopior. Även de skärpta bestämmelserna om behandlingen av känsliga personuppgifter, som avvikande från den gällande lagen innefattar fingeravtryck och DNA-uppgifter, medför kostnadskonsekvenser. En utredning som gjorts i samarbete med de personuppgiftsansvariga visar på följande direkta ekonomiska konsekvenser:

Polisstyrelsen. Skyldigheten att lagra uppgifter om personkategorier som hänför sig till brottmål separat grundar sig delvis på en tidigare rekommendation av Europarådet, och detsamma gäller skyldigheten att separera uppgifter som grundar sig på en personlig bedömning från verifierade uppgifter. Dessa skyldigheter innefattar också en viss mån av flexibilitet. Kraven gör sig huvudsakligen gällande i polisens informationssystem, som hänför sig till behandling av brottmål, och de uppskattas inte medföra några direkta kostnadskonsekvenser. I polisens nya informationssystem ska kraven uppfyllas i samband med revideringsprojekt inom tidtabellen för deras genomförande. Även när det gäller PNR-system enligt det 2:a lagförslaget ska konsekvenserna beaktas till behövliga delar i samband med att systemet utvecklas.

Direkta ekonomiska konsekvenser orsakas av de särskilda krav som hänför sig till behandlingen av personuppgifter (informationsskyldigheter, begränsningar som gäller utlämnande av uppgifter) och de krav i direktivet som gäller rättelse, radering och begränsning av behandling av personuppgifter, till den del dessa inte har uppfyllts tidigare. Kraven ingår redan i det gällande dataskyddsrambeslutet. I samband med genomförandet av dataskyddsdirektivet ska det bedömas i vilken mån begränsningsmarkeringar behöver göras, och hur skyldigheten kan fullgöras på ett så kostnadseffektivt sätt som möjligt. Den gällande lagen innehåller inget krav på begränsning av uppgiftsbehandling, utan i stället är det möjligt att bevara felaktiga personuppgifter parallellt med de rättade uppgifterna. En del krav är tekniskt sett svåra att genomföra eller t.o.m. omöjliga att genomföra fullt ut, och kostnadskonsekvenserna kan vara betydande. Kostnadskonsekvenserna uppskattas uppgå till högst cirka 500 000 euro, beroende på i vilken omfattning ändringarna genomförs.

I fråga om PNR-systemet kan kraven uppfyllas inom ramen för finansieringen av och tidtabellen för systemprojektet. Konsekvenserna hänför sig i detta fall särskilt till skyddet av personuppgifter i situationer där uppgifter lämnas ut, automatiserade beslut, brottsanalys och profilering, samt maskeringen av personuppgifter inom sex månader efter att de har mottagits, även med beaktande av den stora mängd personuppgifter som ska behandlas. Konsekvenserna för informationssystemen följer delvis direkt av genomförandet av PNR-direktivet och delvis av iakttagandet av de krav som ställs i dataskyddsdirektivet.

Vad gäller kraven på inbyggt dataskydd och dataskydd som standard samt andra krav på säkerhet vid behandlingen av personuppgifter som ställs redan i den gällande lagstiftningen om dataskydd har strävan varit att bygga upp polisens informationssystem så att de bedöms uppfylla kraven enligt direktivet. Till denna del får kraven enligt direktivet inga direkta ekonomiska konsekvenser. Det är dock möjligt att praxis måste ändras till följd av de nya skärpta bestämmelserna, varvid skäliga kostnadskonsekvenser kan uppstå. Dessa konsekvenser hänför sig i synnerhet till kränkningar av informationssäkerheten och garderingen mot dessa samt till

riskbedömningen i anslutning till behandlingen av personuppgifter. Eventuella ändringar ska genomföras efter den personuppgiftsansvariges eget omdöme, och de ekonomiska konsekvenserna av dessa uppskattas uppgå till högst cirka 500 000 euro. Däremot uppskattas de nya kraven i EU-lagstiftningen som gäller skyldigheten att underrätta en annan personuppgiftsansvarig om kränkningar av informationssäkerheten medföra kostnadskonsekvenser, som kan variera avsevärt (sammanlagt från 100 000 euro till 2 miljoner euro). Beträffande PNR-systemet beaktas kraven inom ramen för finansieringen av och tidtabellen för systemprojektet.

Förutom markeringar för begränsad användning bedöms i synnerhet de krav i direktivet som gäller behandlingen av loggar få betydande kostnadskonsekvenser inom EU för en stor del av de personuppgiftsansvariga. Av denna orsak har också en övergångsperiod på sju år införts i direktivet när det gäller fullgörandet av skyldigheterna. Logguppgifter samlas redan in i omfattande grad, och bestämmelsen i direktivet innehåller också en viss flexibilitet. När det gäller polisens informationssystem beror kostnadskonsekvenserna på hur strikt kravet på logguppgifter i systemförfrågningar tolkas. Den personuppgiftsansvarige kan också efter eget omdöme höja kravet på loggens exakthet. Som helhet kan man dock uppskatta att eventuella ändringsbehov i anslutning till loggningskraven kan uppfyllas så att de ekonomiska konsekvenserna förblir skäliga och uppgår till högst 250 000 euro. I samband med nya systemprojekt, såsom Vitja-projektet, ska skyldigheterna beträffande loggar beaktas.

Centralkriminalpolisen. I fråga om centralen för utredning av penningtvätt uppskattas de ekonomiska konsekvenserna för informationssystemen som helhet bli skäliga. Kostnadskonsekvenserna fördelar sig med hänseende till fullgörandet av de olika skyldigheterna så att de ekonomiska konsekvenserna av eventuella nödvändiga ändringsarbeten som helhet varierar från några tiotusen euro till hela 1 miljon euro. Det är också möjligt att tillämpa den flexibilitet som direktivet tillåter på de informationssystem som centralen för utredning av penningtvätt använder. En annan omständighet som medger flexibilitet är att alla uppgifter i penningtvättsregistret inte rör brottsmisstankar, vilket innebär att kravet på att uppgifter som hänför sig till olika personkategorier ska separeras från varandra till behövliga delar ska tillämpas när det är fråga om ett brottmål och personernas ställning behöver antecknas i registret. De nödvändiga ändringarna i informationssystemen kan till stor del genomföras till skäliga kostnader. Centralen för utredning av penningtvätt behöver dock göra vissa ändringar i informationssystemen även till följd av genomförandet av ändringarna i det fjärde penningtvättsdirektivet. Beträffande penningtvättsregistret har det uppskattats att en del av den personuppgiftsansvariges uppgifter också i viss mån medför konsekvenser för användningen och administrationen av informationssystemet.

Skyddspolisen. Behandlingen av personuppgifter vid skyddspolisen regleras av en allmän lag, närmare bestämt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Hänvisningen till en lag som bygger på dataskyddsdirektivet medför i stor utsträckning samma krav på skyddspolisen som på andra myndigheter som hör till direktivets tillämpningsområde när det gäller behandlingen av personuppgifter, exempelvis skyldigheten att om möjligt specificera personens ställning i registret. I och med de informationssystemsprojekt som redan genomförts och som pågår för tillfället uppskattas det emellertid att skyddspolisens informationssystem redan uppfyller kraven i den nya dataskyddslagstiftningen. Systemen behöver således inte ändras i någon betydande grad. De krav som följer av lagprojekten beaktas inom ramen för finansieringen av och tidtabellen för systemprojekten. Exempelvis de krav som ställs i den föreslagna lagstiftningen, nämligen kravet att separera uppgifter som grundar sig på en personlig bedömning från verifierade uppgifter, de särskilda informationsskyldigheterna, begränsningarna i anslutning till utlämnande av uppgifter samt kraven på att markera rättelse, radering och begränsad behandling av personuppgifter, kan anses bli uppfyllda senast när de pågående systemprojekten upphör. Det bör dock noteras att om

tillämpningspraxisen enligt det nya lagpaketet om dataskydd ställer betydligt striktare krav på personuppgiftsbehandlingen vid skyddspolisen kan kostnaderna öka avsevärt.

Skyddspolisens funktionella informationssystem är föremål för ett exceptionellt allvarligt intresse för olagligt inhämtande av information. Beträffande inbyggt dataskydd och dataskydd som standard har skyddspolisens informationssystem genomförts så att de bedöms uppfylla de särskilda krav som ställs på dem när det gäller kränkningar av informationssäkerheten och beredskap inför sådana. Sannolikt blir det dock nödvändigt att göra vissa ändringar i de övriga informationssystemen. Följaktligen uppskattas administreringen av integreringarna föranleda anslutnings- och utrustningskostnader till ett belopp av cirka 150 000 euro samt i en betydande omfattning även arbetskraft. Beroende på vilka ändringsarbeten som krävs uppskattas arbetskraftsinsatsen uppgå till 75 000–300 000 euro per år.

Dataskyddsförordningen

Polisstyrelsen. Polisstyrelsen ansvarar för registerföringen i anslutning till de informationssystem som hör till dataskyddsförordningens tillämpningsområde. Polisens befintliga informationssystem har byggts upp så att de till stor del redan uppfyller de krav på inbyggt dataskydd, dataskydd som standard och säker personuppgiftsbehandling som anges i dataskyddsförordningen. Kostnadskonsekvenser kan dock uppstå om uppdateringen av de gemensamma anvisningarna om och kraven på informationssäkerhet inom statsförvaltningen eller ändringar i hotbedömningarna i anslutning till uppgiftsbehandlingens säkerhet leder till att systemen behöver ändras. De konsekvensbedömningar som krävs enligt artikel 35 i dataskyddsförordningen kan dessutom medföra kostnader, om de leder till att skyddsåtgärder måste utvecklas för informationssystemsapplikationerna.

De största direkta kostnadskonsekvenserna av förordningen när det gäller registerapplikationer som administreras för ändamål som tjänar tillståndsförvaltningen och relaterade tillsynsändamål uppstår för den registrerade till följd av den i artikel 18 angivna rättigheten att kräva att behandlingen av personuppgifterna begränsas samt för den personuppgiftsansvarige till följd av den i artikel 19 angivna skyldigheten att underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Kostnader föranleds också av den registrerades möjlighet att på elektronisk väg begära att få utnyttja sina rättigheter och av den registrerades rättighet att få de begärda uppgifterna i en allmänt tillämplig elektronisk form.

En del av konsekvenserna för informationssystemen överensstämmer med konsekvenserna av dataskyddsdirektivets genomförande. En del av kraven kan uppfyllas inom ramen för de pågående systemprojekten, vilket minskar kostnadskonsekvenserna. De exakta kostnadskonsekvenserna beror också på hur strikt kraven i dataskyddsförordningen tolkas. Kostnaderna för ändringar i informationssystemen som görs enligt den mest strikta tolkningen kan bli ansenliga och förutsätta betydande tilläggsfinansiering.

Nationella regleringslösningar

Konsekvenser för informationssystemen. Av de nationella regleringslösningarna orsakar utvidgningarna i fråga om behandlingen av personuppgifter i 2 kap. i det 1:a lagförslaget bland de största direkta konsekvenserna för informationssystemen. Konsekvenserna kan emellertid till stor del täckas med projektfinansiering bl.a. i samband med Vitja-projektet. Den största ändringen på informationssystemsnivå hänför sig till den föreslagna paragrafen om behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning i 2 kap., som i praktiken innebär att personregistrets innehåll utvidgas och att informationssystemet tekniskt sett avvi-

ker från det nuvarande informationssystemet för misstänkta. Kostnaderna för systemet för kriminalunderrättelseinhämtning täcks till alla delar med Vitja-projektfinansiering, varför dessa kostnader inte bedöms i närmare detalj i detta sammanhang.

Förutom det föreslagna 2 kap. medför också de ändringar som föreslås i bestämmelserna om utplåning betydande konsekvenser för informationssystemen. Genom de lagändringar som gjordes år 2013 (RP 66/2012 rd) ändrades bestämmelserna om utplåning av personuppgifter i linje med förändringarna i omvärlden. I lagändringen infördes en övergångsperiod på fyra år, eftersom en revidering av informationssystemet för polisärenden planerades. Ändringarna i bestämmelserna om utplåning medförde stora kostnader, och följaktligen var det inte ändamålsenligt att genomföra dem i det gamla systemet. I och med att tidtabellen för genomförandet av Vitja-projektet ändrats och en ny bedömning av bestämmelserna om utplåning inletts i samband med beredningen av det 1:a lagförslaget ska övergångsperioden för den lagändring som trädde i kraft år 2014 förlängas med två år, dvs. till den 1 januari 2020, i fråga om 22 §, som gäller utplåning av uppgifter ur informationssystemet för polisärenden (RP 181/2017 rd). Det föreslås att bestämmelserna om utplåning i kap. 5 i det 1:a lagförslaget i propositionen ska ändras. Exakt vilka konsekvenser för informationssystemen de föreslagna nya ändringarna får i förhållande till de tidigare har inte kunnat bedömas i detta skede.

Dessutom uppstår det i fråga om bestämmelserna om utlämnande av personuppgifter direkta konsekvenser för informationssystemen även av den föreslagna bestämmelsen om utlämnande av personuppgifter som rör ett tillstånds giltighet genom elektronisk kommunikation till privata sammanslutningar och näringsidkare. Till den del det är fråga om innehavare av näringstillstånd i vapenbranschen kompletterar bestämmelserna de ändringar i skjutvapenlagen som föranleder kostnadskonsekvenserna. I paragrafen begränsas dock inte de privata sammanslutningar och näringsidkare som hör till dess tillämpningsområde. Det har således i detta skede inte varit möjligt att bedöma i vilken mån bestämmelserna medför konsekvenser för polisen med avseende på informationssystemen. Bestämmelsen innebär att uppgifter får lämnas ut till ett begränsat antal mottagare via en elektronisk tjänst som begränsas med hjälp av administrering av användarrättigheter. Det har dock inte uppskattats hur stort antal mottagare det kan vara fråga om.

Tillståndsförvaltningsuppgifter och relaterade tillsynsuppgifter. Genom att behandlingsändamålen i anslutning till tillståndsförvaltning utökas med uppgifter enligt hittegodslagen blir det möjligt att i ett riksomfattande personregister behandla sådana personuppgifter i anslutning till hittegodsverksamhet som behandlats i enhetsspecifika registerapplikationer i enlighet med den gällande lagen. Inrättandet av en eventuellt ny registerapplikation medför informationssystemskostnader som dock inte kan anses följa direkt av ändringarna i personuppgiftslagen för polisväsendet eller den övriga dataskyddslagstiftningen. [*Kompletteras i samband med den fortsatta beredningen*.]

Tekniska anslutningar. Det föreslagna 4 kap. innehåller en bestämmelse enligt vilken personuppgifter under vissa förutsättningar kan lämnas ut via en teknisk anslutning. Även den gällande lagen innehåller en sådan möjlighet, men bestämmelserna har justerats i förhållande till den gällande lagen. Syftet med bestämmelserna är inte att ändra nuläget, och möjligheten att öppna tekniska anslutningar ska vara begränsad till motiverade situationer som kräver att ett separat beslut fattas. Det är således omöjligt att ge en exakt bedömning av konsekvenserna. Samtidigt medför öppnandet av en ny teknisk anslutning vissa kostnadskonsekvenser för polisen. De största kostnadskonsekvenserna och den mest betydande administrativa bördan när det gäller att öppna tekniska anslutningar orsakas dock i dessa situationer av iakttagandet av kraven enligt dataskyddslagstiftningen. Konsekvenserna rör delvis den personuppgiftsansvarige och personuppgiftsbehandlingen och delvis informationssystemen. Den personuppgiftsansvarige är enligt den nya dataskyddslagstiftningen skyldig att säkerställa att personuppgifterna

skyddas på behörigt sätt oberoende av på vilket sätt de lämnas ut. När en teknisk anslutning öppnas i ett system kan den personuppgiftsansvarige eller personuppgiftsbiträdet inte i alla situationer direkt övervaka vilka personuppgifter som lämnas ut ur systemet. Den personuppgiftsansvarige ansvarar också för att de personuppgifter som lämnas ut är korrekta och aktuella. Dataskyddslagstiftningen medför också konsekvenser för informationssystemen i situationer där behandlingen av personuppgifter har begränsats. I dessa situationer ska den tekniska anslutningen till informationssystemet ordnas så att de obligatoriska kraven enligt dataskyddslagstiftningen kan uppfyllas i dem. Dataskyddslagstiftningen kan få motsvarande konsekvenser också för sådana tekniska anslutningar som öppnats redan tidigare. Konsekvenserna för informationssystemen har i fråga om dataskyddslagstiftningen till övriga delar bedömts noggrannare ovan.

PNR-direktivet

De ekonomiska konsekvenserna av PNR-direktivet för myndigheterna har bedömts i samband med beredningen av direktivet i en U-skrivelse som statsrådet överlämnat till riksdagen (U 66/2010 rd) och i kompletterande skrivelser. PNR-direktivet genomförs genom det 2:a lagförslaget i propositionen. I kommissionens konsekvensbedömning har två tekniska modeller jämförts med avseende på informationssystemen; å ena sidan en decentraliserad informationssystemslösning där varje medlemsstat huvudsakligen ansvarar för de ändringar som ska göras i informationssystemen och för administrationen av systemen, å andra sidan ett centraliserat informationssystem på EU-nivå som medför resurskonsekvenser för både medlemsstaternas myndigheter och den centraliserade enheten, men vars kostnader täcks med medel ur EU:s budget. Den decentraliserade lösning som omfattats i direktivet innebär att huvuddelen av konsekvenserna för informationssystemen och resurskonsekvenserna orsakas de nationella myndigheterna. I konsekvensbedömningen har två alternativ jämförts. I det första alternativet begränsas direktivet till att gälla enbart flygtrafik över EU:s yttre gränser, och i det andra utvidgas det till att gälla även flygtrafik inom EU. Alternativet att begränsa direktivet till flygtrafik över de yttre gränserna medför mindre kostnadskonsekvenser för myndigheterna. De brottsbekämpande myndigheterna orsakas dock kostnader för uppbyggandet av informationssystemet och olika detaljer i anslutning till detta, som bygger på kraven i direktivet, inklusive systemgränssnitten. De övriga konsekvenserna rör särskilt lagringen av personuppgifter och utplåningen av känsliga personuppgifter, anonymiseringen av personuppgifter, utlämnande av personuppgifter och automatiserade beslut.

Beträffande myndighetskostnader har det konstaterats att utnyttjandet av uppgifter inte utgör en händelse av engångskaraktär utan en del av kontinuerlig brottsbekämpning, vilket gör det svårare att göra en engångsanalys av myndighetskostnaderna. En enhet för passagerarinformation bestående av personal från polisen, Tullen och gränsbevakningsväsendet inledde strukturellt sett sin verksamhet den 1 november 2016 som en del av PTG-strukturen. I mars 2017 arbetade 68 personer vid enheten (polisen 39, Tullen 21 och gränsbevakningsväsendet 8), och de ansvarar också för andra PTG-uppgifter. Enhetens verksamhet grundar sig på den gällande lagens bestämmelser om rättigheterna att få uppgifter om passagerarna och besättningen i de olika reseformerna för PTG-myndigheternas brottsbekämpningsuppgifter.

De kostnader som orsakas myndigheterna har uppskattats i september 2017 inom ramen för projektet för inrättandet av enheten för passagerarinformation. Personalkostnaderna uppskattas preliminärt uppgå till 37 årsverken, och underhållet av de lokaler som personalen utnyttjar uppgår till cirka 150 000 euro. Uppskattningen kan innefatta också andra uppgifter än sådana som orsakas direkt av genomförandet av direktivet och av det 2:a lagförslaget. De system som är avsedda för behandling av passageraruppgifter uppskattas orsaka kostnader på cirka 3-4 000 000 euro per år. Kostnaderna för systemet preciseras senare i takt med att projekten framskrider. Beträffande personalkostnaderna bör det noteras att enheten för passagerarinformation

förutom flygpassageraruppgifter också analyserar uppgifter om passagerare och besättning i andra trafikformer i brottsbekämpningssyfte. En del av konsekvenserna för personalresurserna följer således inte direkt av det 1:a eller det 2:a lagförslaget, utan de har uppstått redan i samband med genomförandet av 13 § 1 mom. 16 punkten i den gällande lagen. [*Kompletteras i samband med den fortsatta beredningen*.]

Personuppgiftsansvarig i fråga om de personuppgifter som behandlas av *enheten för passagerarinformation* är Polisstyrelsen. Trots detta medför iakttagandet av kraven i både PNR-direktivet och dataskyddsdirektivet en motsvarande administrativ börda för enheten för passagerarinformation som för de övriga polisenheterna som behandlar personuppgifter. Den administrativa bördan ökar också i och med att det måste beaktas att ändamålet med de personuppgifter som samlats in av lufttrafikföretagen ändras när de överförs till polisens personregister. De ekonomiska konsekvenserna av PNR-direktivet hör nära samman med systemets struktur och dess tekniska genomförande. På nationell nivå kommer genomförandet av direktivet att förutsätta att de behöriga myndigheterna utökar sina personalresurser för behandlingen av uppgifter och analysverksamheten. Ett dataskyddsombud har utnämnts för enheten för passagerarinformation i enlighet med kraven i PNR-direktivet.

4.4 Samhälleliga konsekvenser

Konsekvenser för medborgarnas ställning i samhället och för det civila samhällets verksamhet

Europeiska kommissionen har bedömt i synnerhet vilka konsekvenser dataskyddsförordningen får för enskilda personer. Dataskyddslagstiftningen är i väsentlig grad förknippad med medborgarens ställning i samhället, och syftet med den är att säkerställa att medborgarna kan utöva sina rättigheter när det gäller personuppgiftsbehandling. Den personuppgiftsbehandling som hör till dataskyddsförordningens tillämpningsområde anknyter i det 1:a lagförslaget till tillståndsförvaltning och relaterade tillsynsfrågor. De tillsyns- och tillståndsfrågor som omfattas av dessa bestämmelser överensstämmer huvudsakligen med den gällande lagen, med undantag av de preciserade bestämmelserna om sådan personuppgiftsbehandling som hänför sig till tillsyn enligt lagen om penningtvätt och tillsyn enligt lotterilagen samt de ändringar som rör hittegodsverksamheten. Med beaktande av att dataskyddsförordningen får obetydligare konsekvenser för myndigheternas personregister och att tillämpningsområdet för 1995 års direktiv i Finland nationellt har utvidgats till att gälla all behandling av personuppgifter, orsakas konsekvenserna för personuppgiftsbehandlingen i anslutning till polisens tillståndsärenden främst av de mer detaljerade bestämmelserna.

Det faktum att den registrerades rättigheter betonas kraftigare än tidigare i dataskyddsförordningen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten kan förväntas förbättra medvetenheten på så sätt att de registrerade de facto kan utnyttja sina rättigheter i förhållande till personuppgifter som samlats in för de behandlingsändamål som anges i 2 kap. i det 1:a lagförslaget. När det gäller personuppgiftsbehandling i anslutning till brottmål innefattar dock både det 1:a och det 2:a lagförslaget inskränkningar av den registrerades rätt till insyn i fråga om vissa behandlingsändamål, vilket med avseende på den nya typen av personuppgiftsbehandling (kriminalunderrättelseinhämtning, passageraruppgifter) till vissa delar medför en mer omfattande inskränkning av integritetsskyddet. I fråga om dessa behandlingsändamål kan den registrerade endast utnyttja sin rätt till insyn indirekt via dataskyddsmyndigheten. Vilka konsekvenser de föreslagna inskränkningarna får med tanke på tillgodoseendet av de grundläggande fri- och rättigheterna enligt grundlagen bedöms närmare i 4 kap.

Även betoningen av den personuppgiftsansvariges ansvar kan uppskattas ha en positiv inverkan på hur integritetsskyddet och individens rättigheter tillgodoses i polisens tillståndsförvalt-

ningsärenden när det gäller sådan behandling av personuppgifter som hör till dataskyddsförordningens tillämpningsområde. Dessutom är den personuppgiftsansvarige i regel skyldig att informera den registrerade om kränkningar av informationssäkerheten, vilket stärker den registrerades ställning.

Å ena sidan är en målsättning med det 1:a lagförslaget att underlätta polisens gränsöverskridande samarbete med de brottsbekämpande myndigheterna i EU-medlemsstaterna. Det faktum att dessa i lagförslaget jämställs med finländska personuppgiftsansvariga i enlighet med den nya dataskyddslagstiftningen kan leda till ett effektivare utbyte av personuppgifter än tidigare. Överföringar av personuppgifter mellan behöriga myndigheter i EU-medlemsstaterna kan redan i sig göra det svårare för personerna att utnyttja sin rätt till dataskydd och i synnerhet att skydda sina personuppgifter från illegal användning eller illegalt utlämnande, men ännu svårare blir det när personuppgifter överförs till stater utanför unionen. Även en finländsk personuppgiftsansvarig har sämre möjligheter att övervaka hur uppgifterna används i dessa situationer trots att regleringen skärpts. Den personuppgiftsansvariges och dataskyddsmyndighetens befogenheter är otillräckliga i synnerhet i sådana fall där behandlingen av personuppgifter anknyter till verksamhet utanför statens gränser. I EU-lagstiftningen om dataskydd har man fäst vikt vid behovet av att främja ett intensivare samarbete mellan dataskydds- och tillsynsmyndigheterna, för att dessa vid behov ska kunna utbyta uppgifter med sina utländska samarbetspartner. Genom detta kan man i viss mån främja tillgodoseendet av den registrerades rättigheter. Strävan har varit att säkerställa dessa rättigheter i dataskyddslagstiftningen och det 1:a lagförslaget genom att ställa mer strikta kriterier för överföringar av personuppgifter till tredjeländer. Å andra sidan har den registrerades rättigheter säkerställts i dataskyddslagstiftningen när det gäller verksamhet inom EU:s gränser genom att dataskyddsmyndigheterna getts befogenheter som överskrider medlemsstatens gränser. Syftet med bestämmelserna har också varit att göra det lättare för den registrerade att utnyttja sina rättigheter i detta avseende. Den registrerades användning av sina rättigheter förbättras dessutom av att bestämmelserna om rätten till effektiva rättsmedel är mer detaljerade än tidigare.

I 4 kap. i det 1:a lagförslaget finns uttryckliga bestämmelser som gör det möjligt att lämna ut personuppgifter till allmänheten. Syftet med dessa bestämmelser är att på motsvarande sätt som bestämmelserna i den gällande personuppgiftslagen för polisväsendet möjliggöra s.k. offentliga efterlysningar, varvid allmänhetens hjälp utnyttjas för att nå efterlysta personer. Dessa möjligheter har man redan tidigare strävat efter att utnyttja i allt högre grad, och de har ofta visat sig vara effektiva. Även dessa bestämmelser ger det civila samhället en allt starkare roll som ett stödjande element i polisens arbete. Samtidigt har bestämmelserna en inskränkande effekt på integritetsskyddet för den person vars personuppgifter behandlas, med beaktande av att personuppgifterna i dessa situationer sprids snabbt och i stor utsträckning.

Vidare har polisen med stöd av 2 kap. rätt att behandla uppgifter som grundar sig på observationer som gjorts av polismän samt tipsuppgifter från allmänheten. Denna typ av personuppgifter ska behandlas som observationsuppgifter. Med stöd av 2 kap. 6 §, som ersätter bestämmelsen om observationsuppgifter i den gällande lagen, kan uppgifter även i fortsättningen registreras, om uppgifterna i fråga med fog kan bedömas ha samband med brottslig verksamhet. Polisen kan också med stöd av det föreslagna 4 kap. 3 § 2 mom. lämna ut personuppgifter till allmänheten för att få tips.

Ur medborgarnas synvinkel är det också viktigt att det i bestämmelserna om genomförandet av dataskyddslagstiftningen har fästs särskild vikt vid övervakningen av personuppgiftsbehandlingen. Bestämmelserna är mer detaljerade än den gällande allmänt tillämpliga personuppgiftslagen och bestämmelserna i personuppgiftslagen för polisväsendet. Dessa ändringar anses öka förtroendet för den behandling av personuppgifter som utförs av polisen. Det faktum att en angivare eller ett vittne till ett brott eller någon annan person som har samband med

ett brott också själv kan bli införd i polisens personregister för ändamål som tjänar kriminalunderrättelseinhämtning påverkar dock dessa personers ställning. Kriterierna för behandling av personuppgifter som rör angivare och andra som har samband med brott samt övervakningen av personuppgiftsbehandlingen är av särskild vikt när det gäller att säkerställa att medborgarna vågar ange brott för polisen.

De 1:a lagförslagets 2 kap. 9 § innehåller mer detaljerade bestämmelser än tidigare där det föreskrivs om behandlingen av personuppgifter vid övervakning av penningspelsverksamhet enligt lotterilagen. Avvikande från den gällande lagen innefattar bestämmelserna också rätten att till vissa delar behandla personuppgifter som rör enskilda personer, trots att övervakningen är inriktad på penningspelsbolaget. Polisstyrelsens lotteriförvaltning har rätt att behandla personuppgifter som rör enskilda spelare och som ingår i penningspelsbolagets kundregister och spelmaterial till den del det är nödvändigt för att övervakningen ska kunna utföras. Detta påverkar integritetsskyddet för dessa personer. Samtidigt har spelarnas personuppgifter redan i nuläget behandlats som en del av övervakningen, och de faktiska konsekvenserna av det 1:a lagförslaget blir således till denna del obetydliga.

Känsliga personuppgifter behandlas inom polisen för att de polisuppgifter som hör till direktivets och förordningens tillämpningsområde ska kunna skötas. När det gäller känsliga personuppgifter förbättrar de preciserade bestämmelserna den registrerades rättigheter i samband med personuppgiftsbehandling som utförs av polisen. Detta är av betydelse särskilt i sådana fall där det är fråga om biometriska och genetiska uppgifter, som avvikande från den gällande lagstiftningen ska klassificeras som känsliga uppgifter och som således inom direktivets tillämpningsområde kan behandlas endast när det är nödvändigt. Villkoren för behandling av känsliga personuppgifter skärps också inom förordningens tillämpningsområde. Det är i regel förbjudet att behandla sådana personuppgifter som hör till de särskilda kategorier av personuppgifter som avses i artikel 9 i förordningen. Artikel 9.1 i förordningen innehåller en uttömmande förteckning över de undantag med stöd av vilka det är tillåtet att behandla dessa uppgifter. Inom bägge dataskyddsrättsakternas tillämpningsområde ställs också särskilda krav på skyddet av känsliga personuppgifter. I och med det bredare tillämpningsområdet för förenlig behandling av personuppgifter har samtidigt i synnerhet det att fingeravtrycksuppgifter som registrerats med stöd av 131 § i utlänningslagen i vissa fall också kan användas för brottsutredningsändamål en inskränkande effekt på integritetsskyddet.

I 4 kap. i lagförslaget beaktas också de ändringar i utlämnandet av känsliga personuppgifter som följt särskilt i takt med EU-lagstiftningens utveckling. Även vid utlämnandet av dessa personuppgifter gäller det att till alla delar beakta de krav som i dataskyddsförordningen och dataskyddsdirektivet ställs på kriterierna för behandling av känsliga personuppgifter och på skyddet av dessa. Känsliga personuppgifter får inom direktivets tillämpningsområde lämnas ut endast när det är nödvändigt för identifieringen av en person. I och med genomförandet av den nya dataskyddslagstiftningen fästs i 9 kap. 1 § särskild vikt vid kraven på behandling av känsliga uppgifter till den del det är fråga om skyddet av dessa personuppgifter, om vilket dataskyddsbestämmelserna också innehåller striktare krav än tidigare.

Konsekvenser för jämlikhet, barn och jämställdhet mellan könen

Konsekvenser för jämlikhet. Det 1:a lagförslaget får som en del av genomförandet av dataskyddsförordningen och dataskyddsdirektivet en indirekt konsekvens för realiseringen av jämlikheten. I artikel 10 i dataskyddsdirektivet föreskrivs om behandlingen av känsliga personuppgifter. De krav som anges i artikeln har beaktats i 2 kap. 2 § och 9 kap. 1 § i lagförslaget. I bestämmelserna förutsätts förutom ett högre behandlingskriterium än i fråga om behandlingen av andra personuppgifter även en högre informationssäkerhetsnivå i de informationssystem där dessa personuppgifter behandlas. Behandling av känsliga personuppgifter tillåts endast ut-

ifrån strikta kriterier, om behandlingen är nödvändig. Med känsliga personuppgifter avses sådana uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

I artikel 11 i dataskyddsdirektivet föreskrivs också om förbud mot så kallad etnisk profilering. Syftet med förbudet är att säkerställa att den registrerade inte blir föremål för ett beslut angående bedömning av personliga aspekter rörande honom eller henne som uteslutande grundas på automatiserad behandling och som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne. Uppgiftsbehandlingen omfattas också av ett krav på lämpliga skyddsåtgärder, inklusive skyldigheten att informera den registrerade om behandlingen och rätten till personlig kontakt. Profilering som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden i enlighet med bestämmelserna om grundläggande fri- och rättigheter. Behandling av genetiska uppgifter får exempelvis inte leda till att grupper i särskilt utsatt ställning diskrimineras i samhället. I praktiken bekräftar bestämmelserna det ovillkorliga förbudet mot diskriminering, som gäller redan på grundval av bestämmelserna om grundläggande fri- och rättigheter. Samtidigt hindrar bestämmelsen ändå inte av polisen utförd profilering av personer som misstänks ha samband med brottslig verksamhet, men den säkerställer att profileringen inte får leda till diskriminering.

På realiseringen av jämlikhet inverkar dessutom indirekt de krav i den nya regleringen som gäller bedömningen av riskerna i anslutning till personuppgiftsbehandlingen, vilken konkretiseras i och med det 1:a lagförslaget. De största riskerna hänför sig till sådan behandling av personuppgifter som kan orsaka fysiska, materiella eller immateriella skador och behandling som kan leda till diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller uppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering, eller annan betydande ekonomisk eller social nackdel. Förutom känsliga personuppgifter kan det uppstå särskilda risker exempelvis i anslutning till personuppgifter rörande sårbara fysiska personer, framför allt barn, eller sådan behandling som inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. Denna typ av behandling omfattar i synnerhet sådan personuppgiftsbehandling som avses i det 2:a lagförslaget, men också eventuella jämförelser mellan register som hänför sig till tillämpningen av det 1:a lagförslaget. Vidare kan i synnerhet sådan behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning ha betydelse för realiseringen av jämlikheten, beroende på om personuppgiftsbehandlingen rör en enskild person eller personkategorier. Till denna del har konsekvenserna dock inte bedömts i någon större detalj.

Samtidigt främjas realiseringen av jämlikheten mer allmänt av den harmoniserade EU-regleringen, som garanterar att alla registrerade står i jämlik ställning inom EU när det gäller användningen av sina rättigheter som registrerad. I och med de nya bestämmelserna gäller lika höga krav i alla EU-medlemsstater i fråga om den registrerades rätt till insyn och dataskyddsmyndighetens övervakning av denna. Rättigheterna effektiviseras också av bestämmelserna om administrativa påföljder, som kan följa bl.a. av att den registrerade förvägras rätten att övervaka behandlingen av sina egna personuppgifter.

Konsekvenser för barn. I ingressen till EU:s dataskyddsförordning fästs vikt vid att barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd ska tillämpas i synnerhet när det gäller användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds di-

rekt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn ska inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn. Dessa åtgärder kan, i kombination med de bestämmelser som föreslås för polisen i det 1:a lagförslaget och som effektivare än tidigare stöder förebyggande, avslöjande och utredning av IT-relaterad brottslighet, få en indirekt konsekvens som förbättrar barnets ställning även vid förebyggandet av brott. Barn anses också vara särskilt utsatta för brott som sker online. Samtidigt begår också minderåriga och unga gärningsmän numera en stor del av sina brott online. Exempelvis olika typer av mobbning och trakasserier samt ärekränkningar begås allt oftare online. Samtidigt pekar statistiken på att exempelvis antalet illegala nedladdningar har minskat under de senaste två åren.

Både dataskyddsförordningen och dataskyddsdirektivet fastställer att den personuppgiftsansvarige är skyldig att på klarspråk informera de registrerade om deras rättigheter med särskild hänsyn till sårbara grupper, såsom barn. Denna skyldighet konkretiseras i samband med tillämpningen av det 1:a lagförslaget. Enligt finsk lagstiftning handlar det i regel om alla personer under 18 år. Skyldigheterna för den personuppgiftsansvarige gäller även polisen i sådana fall där den registrerade exempelvis är ett minderårigt brottsoffer, en person som gjort sig skyldig till en brottslig handling eller en tillståndssökande.

I 5 kap. 1 § i det 1:a lagförslaget, som gäller utplåning av personuppgifter, beaktas minderåriga personer som gjort sig skyldiga till en brottslig handling på samma sätt som i den gällande personuppgiftslagen för polisväsendet. Uppgifter om minderåriga personer får inte förvaras lika länge som personuppgifter om myndiga. På så sätt strävar man efter att begränsa de negativa effekter som personuppgiftsbehandling i anslutning till ett brott kan få på ett barns liv, med beaktande av principen om barnets bästa. Med hänsyn till barnets boende, smidiga vardag och mänskliga relationer beaktar lagförslaget också behoven av personuppgiftsbehandling i sådana situationer där man strävar efter att ingripa i unga återfallsförbrytares situation med andra metoder än straffrättsliga medel och på så sätt att förebygga nya brott. Med tanke på dessa situationer föreslås det i enlighet med barnets bästa att uppgifter ska kunna lämnas ut till de sociala myndigheterna i barnskyddssituationer och i syfte att förebygga brott på motsvarande sätt som i de gällande bestämmelserna.

Konsekvenserna för de grundläggande fri- och rättigheterna bedöms till övriga delar i 4 kap. Denna typ av konsekvenser rör i synnerhet skyddet för privatlivet, men också jämlikheten och rättsskyddet.

Konsekvenser för brottsbekämpningen och säkerheten

Syftet med bestämmelserna i EU:s dataskyddsförordning och dataskyddsdirektivet och lagstiftningen om genomförandet av dessa är att underlätta polisens arbete genom att ge akt på de mer omfattande behoven av personuppgiftsbehandling i anslutning till förändringarna i den operativa miljön och säkerhetsläget. Vidare ska de nya bestämmelserna påverka informationssäkerheten och säkerheten i informationssystemen som helhet så att brott som riktas mot dessa kan förebyggas. Denna typ av brott har blivit vanligare, och de kan orsaka betydande olägenheter och skador. Europeiska kommissionen har i sin konsekvensbedömning av dataskyddslagstiftningen fäst vikt vid att verksamhet på nätet utsätter individer, också barn, bl.a. för skadat anseende, ekonomiska skador och rentav fysiska skador, som kan orsakas t.ex. av att uppgifter om individens hälsotillstånd publiceras utan hans eller hennes samtycke eller av trakasserier på nätet. De ekonomiska skador som orsakas av identitetsstölder har på EU-nivå uppskattats uppgå till sammanlagt 700 miljoner euro per år. Under de senaste åren har också allt allvarligare kränkningar av informationssäkerheten vid personuppgiftsbehandling förekommit. Även i Finland har man uppmärksammat allt fler former av brott som riktar sig mot och begås med hjälp av informationsteknik (Källa: Institutet för kriminologi och rättspolitik, Katsauksia

22/2017 - Rikollisuustilanne 2016). Den skärpta dataskyddsregleringen och polisens effektivare rättigheter att behandla personuppgifter kan anses erbjuda bättre verktyg för att förebygga brott som begås på nätet och kränkningar av informationssäkerheten i fråga om personuppgifter, vilket även tjänar polisens målsättningar.

Dataintrång som riktas mot företags och andra organisationers informationssystem anmäls inte nödvändigtvis alltid till polisen. Samtidigt kan det vara nödvändigt att informera kunderna i synnerhet om överbelastningsattacker (Källa: Institutet för kriminologi och rättspolitik, Katsauksia 22/2017 - Rikollisuustilanne 2016). Den nya dataskyddslagstiftningen medför emellertid en större skyldighet att anmäla kränkningar av informationssäkerheten till dataskyddsmyndigheten och de registrerade, vilket kan leda till att dessa gärningar, som hittills förekommit delvis som dold brottslighet, avslöjas oftare än tidigare. Samtidigt ställs det i dataskyddslagstiftningen också hårda krav på inbyggt dataskydd och dataskydd som standard samt informationssäkerhet i informationssystemen, varvid också förebyggandet av brottslighet kan effektiviseras.

Medborgarna är allt aktivare på nätet. Både företagen och de som använder deras tjänster behandlar i stor skala personuppgifter i datanätstjänster. Samtidigt begås en allt större del av brotten på nätet, och gärningsmännen har bättre möjligheter än tidigare att snabbt dölja sina spår. Av dessa orsaker innehåller 2 kap. i det 1:a lagförslaget i propositionen bestämmelser som bedöms främja en effektiv kriminalunderrättelseinhämtning som en del av arbetet med att förebygga, avslöja och utreda brott. Konsekvenser som anknyter till förebyggande av brottslighet och brottsutredning uppskattas följa tydligare av lagstiftningen om polisens befogenheter, och det är därför omöjligt att bedöma vilka faktiska konsekvenser de föreslagna nya bestämmelserna om personuppgiftsbehandling i anslutning till kriminalunderrättelseinhämtning får. Bestämmelserna bedöms dock förbättra polisens möjligheter att få information om brott. Syftet med de föreslagna bestämmelserna är att erbjuda effektiva medel för att gripa gärningsmän och klarlägga deras verksamhet och för att bättre kunna förutse eventuella hotfulla situationer. Målet är att de effektivare möjligheterna att behandla personuppgifter ska främja avslöjandet av brott och öka gärningsmännens risk att bli gripna. Samtidigt ska också dataskyddet och rättsskyddet för angivare och andra utomstående som har samband med ett brottmål säkerställas, så att viljan att anmäla brott inte försvagas, genom att en högre tröskel för registrering av personuppgifter föreslås för dessa personkategorier när det gäller ändamål som tjänar kriminalunderrättelseinhämtning.

Enligt Europols hotbedömning av gränsöverskridande och grov brottslighet 2017 är en av de största hotbilderna inom EU olika typer av brottslighet på nätet. Bestämmelserna om utlämnande av personuppgifter till andra myndigheter och till privata sammanslutningar och näringsidkare i 4 kap. i det 1:a lagförslaget har justerats för att säkerställa att bestämmelserna i ljuset av hotbilderna och statistiken över brottsligheten möter polisens nuvarande behov. Genom att myndigheterna garanteras tillräckliga rättigheter att lämna ut personuppgifter till varandra ökar direkt möjligheterna att avslöja och utreda brott samt risken för gärningsmän att bli gripna. Samtidigt ingår det i 4 kap. i lagförslaget en uttrycklig bestämmelse om att polisen i begränsad utsträckning får lämna ut personuppgifter i brådskande fall även till privata sammanslutningar och näringsidkare i synnerhet för att bekämpa brottslighet på nätet. På så sätt möjliggörs ett smidigt samarbete mellan polisen och företagen. Det föreslås att en motsvarande bestämmelse ska ingå i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten till den del det är fråga om företag som är belägna i tredjeländer. Syftet är att genom snabbt och direkt samarbete och mer omfattande personuppgiftsbehandling i anslutning till kriminalunderrättelseinhämtning effektivare än tidigare kunna förebygga, avslöja och utreda brott som begås på nätet.

Samtidigt är strävan också att genom den nya dataskyddslagstiftningen bekämpa personregisterbrott och annan osaklig behandling av personuppgifter, vilket i allmänhet har en säkerhetsupprätthållande effekt. Brist på övervakning och skydd ökar risken för exempelvis intrång i register. Den nya lagstiftningen fäster särskild vikt vid kraven på övervakning, rättsmedel och administrativa påföljder, som ska ha en förebyggande effekt med tanke på att övervakningen också förbättrar möjligheterna att avslöja personregisterbrott och ökar risken för gärningsmän att bli gripna.

Genom det 2:a lagförslaget i propositionen eftersträvas kraftigare verkningar än genom det 1:a lagförslaget när det gäller bekämpningen av grov brottslighet, särskilt gränsöverskridande brottslighet. Genom lagförslaget strävar Finland efter att möta de hotbilder som legat till grund för kommissionens förslag till ett PNR-direktiv. Kommissionen har i sin konsekvensbedömning motiverat direktivförslaget med att gränsöverskridande brottslighet är ett växande fenomen i Europeiska unionen och den övriga världen. Som exempel lyfter kommissionen fram i synnerhet människohandel och narkotikabrottslighet, som också Europol tar upp i sin hotbedömning av gränsöverskridande brottslighet (2017). Dessa former av brottslighet har ökat kontinuerligt inom EU. I kommissionens konsekvensbedömning och Europols hotbedömning riktas dessutom fokus i fråga om gränsöverskridande brottslighet på organiserad illegal invandring och smuggling av valuta och varor. De olika formerna av gränsöverskridande brottslighet utgör ett allvarligt hot mot samhället och de ekonomiska strukturerna, och de medför kostnader för staten även med beaktande av de åtgärder som krävs för brottsbekämpningen. Brotten orsakar också skada och lidande för offren.

Kommissionen har fäst vikt vid att de flesta formerna av gränsöverskridande brottslighet också är förknippade med resor över gränserna. I synnerhet människosmuggling och organiserad illegal invandring omfattar tredjelandsmedborgare som smugglas in till EU, men även narkotikasmuggling är förknippad med resor över gränserna. Även terrorister och andra som bedriver kriminell verksamhet rör sig över gränserna. Ett mål med PNR-direktivet är att utöka urvalet av medel för att bekämpa terrorism och övrig grov brottslighet. Till denna del bör det dock noteras att terroristerna och den organiserade brottsligheten delvis opererar inom statens gränser. Vidare bör det noteras att PNR-direktivet endast gäller behandling av flygpassagerares personuppgifter, medan en del av den gränsöverskridande passagerartrafiken utgörs av sjöfart och järnvägstrafik.

Målsättningen med det 2:a lagförslaget i propositionen är att säkerställa att de brottsbekämpande myndigheterna har tillgång till så mycket information som möjligt om de ovan avsedda personernas resor samt att förbättra förutsättningarna för informationsutbyte mellan dessa myndigheter när det gäller flygpassageraruppgifter. Detta bedöms effektivisera bekämpningen av gränsöverskridande brottslighet. I Finland har polisen redan med stöd av den gällande personuppgiftslagen för polisväsendet rätt att få passageraruppgifter av trafikföretag. Den gällande bestämmelsen gäller inte bara lufttrafikföretag, utan också andra trafikformer. Det 2:a lagförslaget i propositionen gör det emellertid möjligt med stöd av direktivet att registrera personuppgifter om alla flygpassagerare för en längre tid, medan den gällande lagen endast gör det möjligt att i enskilda fall jämföra passageraruppgifter med uppgifterna i polisens personregister. Lagförslaget möjliggör dessutom jämförelse av flygpassageraruppgifter redan före avgång, vilket kan anses erbjuda ett effektivare medel för bekämpning av gränsöverskridande brottslighet än tidigare. EU-medlemsstaternas gällande reglering om insamling och utnyttjande av passageraruppgifter för brottsbekämpningsändamål har i kommissionens konsekvensbedömning ansetts vara oenhetlig. I ljuset av kommissionens bedömning effektiviseras utbytet av uppgifter mellan myndigheterna också genom att de personuppgifter som med stöd av det 2:a lagförslaget och de övriga EU-medlemsstaternas genomförandelagstiftning samlas in om passagerarna är enhetligare och i större skala än tidigare tillgängliga för brottsbekämpningsändamål.

PNR-uppgifter (Passenger Name Record) är till sin karaktär overifierade personuppgifter som lämnats av passagerarna själva i motsats till s.k. API-uppgifter (Advance Passenger Information), som grundar sig på uppgifterna i passagerarens pass. PNR-uppgifter utnyttjas huvudsakligen för ändamål som tjänar kriminalunderrättelseinhämtning och i synnerhet för att utforma olika hotbedömningar och riskprofiler. Detta gör det möjligt för brottsbekämpande myndigheter att fokusera sina åtgärder på sådana passagerare som passar in i riskprofilen, i stället för att alla passagerare blir föremål för gränsbevakningsmyndigheternas åtgärder. PNR-uppgifterna blir också tillgängliga för myndigheterna i ett tidigare skede än API-uppgifterna. PNR-uppgifter kan dessutom jämföras med andra personuppgifter som behandlas av myndigheterna, vilket innebär att tillgången till sådan information om en flygpassagerare som behövs för brottsbekämpning effektiviseras, med beaktande av de utmaningar som flygtrafiken inom EU medför. Med hjälp av dessa uppgifter kan man exempelvis få information för brottsanalys om typiska resrutter för personer som smugglar narkotika eller identifiera och utreda kopplingar mellan en resande och en känd brottsling eller kriminell grupp. Enligt det 2:a lagförslaget i propositionen ska det vara möjligt att jämföra PNR-uppgifter med personuppgifter som behandlas i anslutning till brottmål, inklusive sådana ändamål som tjänar kriminalunderrättelseinhämtning och som avses i 2 kap. 4 § i det 1:a lagförslaget.

5 Beredningen av propositionen

5.1 Beredningsskeden och beredningsmaterial

Inrikesministeriet har den 26 januari 2016 tillsatt en arbetsgrupp (SM064:00/2015) som haft till uppgift att sammanställa ett utkast till regeringens proposition med förslag till lag om behandling av personuppgifter i polisens verksamhet. Arbetsgruppen har också utrett och bedömt polisens behov av mer omfattande personuppgiftsbehandling, som föranletts av förändringar i polisens operativa miljö. Mandattiden för projektet förlängdes den 23 maj 2017 så att den löper ut den 28 februari 2018. Företrädare för flera ministerier och myndigheter med behörighet för behandling av brottmål har deltagit i arbetsgruppens arbete. Arbetsgruppen har berett ett utkast till en ny personuppgiftslag för polisväsendet. Utkastet har färdigställts som tjänsteuppdrag vid inrikesministeriet. I samband med projektet har också ett annat lagförslag beretts i syfte att till behövliga delar genomföra Europaparlamentets och rådets direktiv av den 27 april 2016 (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Målet är att regeringspropositionen ska överlämnas till riksdagen så att den i den mån det är möjligt behandlas parallellt med de regeringspropositioner som gäller genomförandet av EU:s dataskyddslagstiftning samt vissa andra lagförslag som gäller behandling av personuppgifter vid myndigheter.

[*Propositionen har varit ute på remiss ... 2017. Den fortsatta beredningen har genomförts som tjänsteuppdrag vid inrikesministeriets polisavdelning.]*

5.2 Remissyttranden och hur de har beaktats

[*Kompletteras efter remissförfarandet.*]

6 Samband med andra propositioner

De ekonomiska och andra konsekvenserna av propositionen följer av EU:s nya dataskyddslagstiftning och det 1:a och 2:a lagförslaget i propositionen som helhet. Propositionen har således samband med det betänkande (52/2017) som beretts av en arbetsgrupp (OM 21/41/2016) som tillsatts av justitieministeriet den 12 januari 2017. Betänkandet innehåller ett utkast till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerhet-

en. Mandattiden för arbetsgruppen var 16.1–29.9.2017. Avsikten är att denna proposition ska överlämnas till riksdagen så samtidigt med justitieministeriets proposition som möjligt. Lagförslagen i propositionen innehåller hänvisningar till den föreslagna lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Propositionen har på motsvarande sätt samband med ett annat förslag som är under beredning, nämligen förslaget till en nationell lagstiftning som kompletterar den allmänna dataskyddsförordningen. Justitieministeriet tillsatte i februari 2016 en arbetsgrupp (TATTI) (OM006:00/2016), som haft till uppgift att bereda de ändringar i den allmänna nationella lagstiftningen om behandlingen av personuppgifter som den allmänna dataskyddsförordningen kräver. Arbetsgruppen har särskilt haft till uppgift att bereda ett förslag till bestämmelser om en nationell dataskyddsmyndighet. Arbetsgruppen överlämnade sitt betänkande den 21 juni 2017.

Även Ålands landskapsregerings utredning om genomförandet av EU-lagstiftningen om dataskydd är relevant för propositionen.

Propositionen har till vissa delar samband med projektet om civil underrättelseinhämtning. Inrikesministeriet tillsatte den 1 oktober 2015 ett projekt (SM47:00/2015) i syfte att bereda förslag till en lagstiftning om civil underrättelseinhämtning. Mandattiden för projektet för civil underrättelseinhämtning gick ut den 28 februari 2017. Genom den föreslagna lagstiftningen om civil underrättelseinhämtning ändras 13 § i den gällande personuppgiftslagen för polisväsendet. Med beaktande av att propositionerna behandlas av riksdagen under en och samma session ska den föreslagna lagändringen under riksdagsbehandlingen samordnas med de motsvarande bestämmelserna i 3 kap. i det 1:a lagförslaget i denna proposition.

Propositionen har dessutom samband med ett annat lagstiftningsprojekt vid inrikesministeriet (SM057:00/2016) som går ut på att bereda en regeringsproposition angående en ändring av lagstiftningen om behandling av personuppgifter vid gränsbevakningsväsendet. Inom projektet bereds ändringar i lagen om behandling av personuppgifter vid gränsbevakningsväsendet till den del de nödvändiga bestämmelserna inte ingår i den nationella lagen om genomförande av dataskyddsdirektivet. Dessutom ska arbetsgruppen bedöma vilka lagändringsbehov som följer av den reviderade EU-lagstiftningen om dataskydd och se över bestämmelserna om behandling av personuppgifter i sjöräddningslagen. Avsikten är att regeringens proposition om den nämnda lagstiftningen ska lämnas till riksdagen samtidigt med denna proposition.

Utöver propositionen om gränsbevakningsväsendet har denna proposition samband med ett arbete som utförs av en arbetsgrupp som tillsatts av finansministeriet (VM059:00/2016). Arbetet går ut på att ändra lagen om behandling av personuppgifter inom Tullen så att den motsvarar den allmänna dataskyddsförordningen och dataskyddsdirektivet till den del de ändringsbehov som följer av direktivet inte täcks genom den allmänna genomförandelagstiftningen i anslutning till dataskyddsdirektivet. Avsikten är att regeringens proposition om den nämnda lagstiftningen ska lämnas till riksdagen samtidigt med denna proposition.

Propositionen har också samband med ett arbete som utförs av en arbetsgrupp som tillsatts av försvarsministeriet (PLM006:00/2016). Arbetet går ut på att bereda en totalreform av lagstiftningen om behandling av personuppgifter inom försvarsförvaltningen. Arbetsgruppen har till uppgift att utreda i vilka avseenden lagstiftningen om behandling av personuppgifter inom försvarsförvaltningen behöver ändras till följd av den reviderade EU-lagstiftningen om dataskydd samt att bereda ett förslag till behövliga författningsändringar. Avsikten är att regeringens proposition om den nämnda lagstiftningen ska lämnas till riksdagen samtidigt med denna proposition.

Även den regeringsproposition som beretts i samband med jord- och skogsbruksministeriets lagstiftningsprojekt (MMM009:00/2017) är relevant med tanke på denna proposition till den del det gäller bestämmelserna om sådan summarisk förundersökning som utförs av jakt- och fiskeövervakare.

I fråga om lagförslagen i alla ovannämnda propositioner ska det säkerställas att hänvisningarna till författningar och paragrafer samt till behövliga delar terminologin samordnas under riksdagsbehandlingen. Därtill är det möjligt att propositionerna innehåller lagförslag som gäller ändringar av samma lagar.

[*Kompletteras innan propositionen överlämnas*.]

DETALJMOTIVERING

1 Lagförslag

1.1 Lag om behandling av personuppgifter i polisens verksamhet

1 kap. **Allmänna bestämmelser**

1 §. *Tillämpningsområde.* I paragrafen anges lagens tillämpningsområde. Lagen föreslås bli tillämpad på helt eller delvis automatiserad behandling av personuppgifter som behövs för skötseln av polisens uppgifter enligt 1 kap. 1 § i polislagen (872/2011) samt på annan behandling av personuppgifter, då personuppgifterna utgör eller är avsedda att utgöra ett personregister eller en del av ett sådant. Till denna del motsvarar förslaget bestämmelsen om tillämpningsområde i den gällande lagen om behandling av personuppgifter i polisens verksamhet.

2 §. *Förhållande till annan lagstiftning.* I 1 och 2 mom. preciseras vilka allmänt tillämpliga författningar och akter om behandling av personuppgifter som ska tillämpas på den behandling av personuppgifter som avses i lagförslaget samt hur tillämpningsområdet är uppdelat. I dagsläget tillämpas personuppgiftslagen som en allmän lag på behandlingen av personuppgifter inom polisen. Ikraftträdandet av EU:s dataskyddspaket differentierar dock rättsgrunden så att det inte längre går att tillämpa en och samma författning på all behandling av personuppgifter. På en del av behandlingen av personuppgifter inom polisen tillämpas dataskyddsförordningen som en allmän rättsakt samt den nationella dataskyddslag som kompletterar den (RP /2017 rd). På största delen av den behandling av personuppgifter som omfattas av tillämpningsområdet för lagförslag 1 tillämpas dock lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (RP /2017 rd), genom vilken dataskyddsdirektivet genomförs.

De bestämmelser i lagförslaget som omfattas av tillämpningsområdet för lagstiftningen om genomförande av dataskyddsdirektivet föreslås bli avgränsade i enlighet med skäl 12 i ingressen till direktivet. I skälet i ingressen sägs att polisens och andra brottsbekämpande myndigheters verksamhet främst är inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, inbegripet polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott. Av bestämmelserna i 2 kap. i lagförslaget är de ändamål med behandlingen som anges i 3–8 § sådana ändamål med behandlingen av personuppgifter som omfattas av direktivets tillämpningsområde.

Enligt det skäl i ingressen som nämns ovan får medlemsstaterna åt behöriga myndigheter anförtro andra uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inklusive att skydda mot och förebygga hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för förordning (EU) 2016/679 (dataskyddsförordningen).

Dataskyddsförordningen gäller polisen som direkt tillämplig lagstiftning. Artikel 6.2 i dataskyddsförordningen gör det dock möjligt att utfärda mer specifika bestämmelser för att anpassa bestämmelserna i förordningen när behandlingen av personuppgifter 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). Artikel 6.3 i dataskyddsförordningen förutsätter att grunden för behandlingen av personuppgifter i dessa situationer ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. För tillämpning av dataskyddsförordningen bör det preciseras för vilken skötsel av polisens i lag föreskrivna uppgifter polisen ska ha rätt att behandla personuppgifter. Uppgifterna föreslås bli preciserade i 2 kap. 9 §. Utöver bestämmelser om ändamålen med behandlingen och de relaterade persongrupperna innehåller lagförslag 1 särskilda bestämmelser för att anpassa reglerna i dataskyddsförordningen till den del det är fråga om utlämnande av personuppgifter, utplåningstider och begränsning av den registrerades rättigheter. När det gäller förenlig behandling av personuppgifter föreslås det att den tillämpliga allmänna författningen bestäms i enlighet med det från det ursprungliga ändamålet med behandlingen avvikande ändamål som personuppgifterna avses bli behandlade för (2 kap. 11 § i lagförslaget).

Behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, inbegripet säkerställande av nationell säkerhet, omfattas inte av dataskyddsförordningens och dataskyddsdirektivets tillämpningsområden. Således faller även bland annat behandlingen av skyddspolisens personuppgifter utanför unionsrätten. Vid beredningen av propositionen har det dock ansetts vara motiverat att jämka samman den reglering som gäller skyddspolisen med behandlingen av andra säkerhetsmyndigheters uppgifter. På behandlingen av skyddspolisens personuppgifter tillämpas enligt förslaget som allmän författning lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten samt i analogi med den gällande lagen som särskild författning polisens nya personuppgiftslag, där skyddspolisen föreslås få ett eget kapitel, 7 kap.

I 3 mom. föreslås en informativ bestämmelse enligt vilken bestämmelser om nödcentralsdatasystemet finns i lagen om nödcentralsverksamhet (692/2010) och bestämmelser om utlänningsregistret finns i lagen om utlänningsregistret (1270/1997).

I 4 mom. föreslås en informativ hänvisningsbestämmelse till lagen om offentlighet i myndigheternas verksamhet (621/1999). Enligt skäl 16 i ingressen till dataskyddsdirektivet påverkar direktivet inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar. Enligt dataskyddsförordningen får personuppgifter i allmänna handlingar som förvaras av en offentlig myndighet eller ett offentligt eller privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med unionsrätten eller medlemsstatens nationella lagstiftning som den offentliga myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter.

3 §. *Definitioner*. Paragrafen motsvarar i huvudsak regleringen enligt den gällande lagen och innehåller nationella definitioner som hänför sig till Schengen- och Europolsamarbetet samt en definition av Eurodacförordningen. På behandlingen av personuppgifter enligt lagförslaget ska i övrigt tillämpas definitionerna i 3 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och i artikel 4 i dataskyddsförordningen.

2 kap. Behandling av personuppgifter

1 §. *Behandling av grundläggande personuppgifter*. I paragrafen föreskrivs det om sådan behandling av grundläggande personuppgifter som föreslås vara tillåten för de ändamål med behandlingen som anges i 2 kap. I 1 mom. föreslås en detaljerad förteckning över sådana grundläggande personuppgifter som till behövliga delar ska få behandlas för de ändamål som anges i 3–5 och 9 §. Med dessa grundläggande uppgifter avses sådana uppgifter för specificering av

en person som får lagras för alla persongrupper när de villkor för behandling som anges i paragraferna är uppfyllda. Förteckningen utgör inget hinder för sådan behandling av i 2 § avsedda andra personuppgifter som anknyter till ärendet vilken hänför sig till de ändamål med behandlingen som anges i 3–5 och 9 §. Som personuppgifter anses uppgifter enligt definitionen i 3 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och i artikel 4 i dataskyddsförordningen. Den föreslagna förteckningen är inte uttömmande utan innehåller en extra kategori av uppgifter, nämligen övriga nödvändiga grundläggande uppgifter som kan jämställas med personuppgifterna i förteckningen och som entydigt kan förknippas med den berörda personen. Förteckningen i 1 mom. hindrar inte att man i anslutning till de grundläggande uppgifterna antecknar specificerande uppgifter om rätt identitet för en person som missbrukat identiteten eller som utsatts för missbruk av identiteten.

I 2 mom. föreskrivs det om personuppgifter som hänför sig till vissa tillståndsärenden och som ska få behandlas utöver de grundläggande uppgifter som preciseras i 1 mom. Dessa personuppgifter utgörs av uppgifter om intressebevakning, försättande i konkurs och meddelande om näringsförbud samt fullgörande av värnplikt.

Bestämmelsen motsvarar i huvudsak innehållet i de uppgifter som enligt den gällande lagen ska lagras i informationssystemet för polisärenden, informationssystemet för förvaltningsärenden och informationssystemet för misstänkta, men samma bestämmelse ska tillämpas på flera ändamål med behandlingen enligt 2 kap. I 3–5 och 9 §, vilka gäller ursprungliga ändamål med behandlingen av personuppgifter, föreslås närmare kriterier för behandlingen av både grundläggande uppgifter och andra personuppgifter som behandlas utöver dem.

2 §. *Behandling av andra personuppgifter som anknyter till det behandlade ärendet.* I 1 mom. beaktas andra sådana uppgifter som polisen behöver behandla i anslutning till det behandlade ärendet eller polisens uppgifter, åtgärder eller händelser och som rör en viss person eller persongrupp. Grundlagsutskottet har ansett att när behandlingen är bunden till en nivå som innebär att den behövs kan det krävas att bestämmelsen är detaljerad. Innehållet i 1 mom. förblir öppet, men de personuppgifter som får behandlas begränsas av att behandlingen ska ingå i ett visst ärende eller en viss uppgift, åtgärd eller händelse och anknyta till något av de ändamål med behandlingen som föreskrivs i 3–5 eller 9 §.

I 1 mom. avsedda uppgifter som anknyter till behandlade ärenden eller polisens uppgifter, åtgärder eller händelser gäller i samband med brottmål och behandling av personuppgifter i anknytning till upprätthållande av allmän ordning och säkerhet framför allt 1) uppgifter i en anmälan om brott eller en anmälan om någon annan händelse, 2) uppgifter om besöksförbud eller skydd för vittnen, 3) uppgifter om fältarbete och i lag särskilt föreskrivna övervakningsuppdrag, 4) uppgifter om tvångsmedel, polisens åtgärder samt olika faser i förundersökning och polisundersökning, 5) behövliga beskrivningar, omständigheter och specificeringar som hänför sig till polisens uppgifter, åtgärder eller händelser, 6) uppgifter som beskriver klassificeringen av gärningsmannen, händelsen eller gärningen samt uppgifter som behövs för sammanlänkning och teknisk undersökning av brott, 7) tillvägagångssätt och medel som har använts eller kan användas för att förbereda och begå brott, 8) de myndigheter som behandlar ärendet och de identifikationsuppgifter de använder för ärendena, 9) identifieringsuppgift om avgörande av åklagare eller domstol och uppgift om någon har dömts till straff, om det fattats beslut om åtalseftergift eller domseftergift, om ett åtal förkastats, lämnats därhän eller avskrivits samt uppgift om ett avgörandes laga kraft, och 10) uppgifter om brott som fåtts av eller via en person, vid behov även personernas förhållande till andra personer.

För sådan behandling av personuppgifter som avses i 9 § är uppgifter som avses i 1 mom. framför allt 1) när det gäller tillstånd uppgifter om ansökan, själva tillståndet, utlåtanden, an-

mälan och beslut, 2) uppgifter om hinder för beviljande eller giltighet av ett tillstånd samt uppgifter för utredning av förutsättningarna för beviljande eller giltighet av ett tillstånd. Med tillstånd avses alla de tillstånd, godkännanden och resedokument medräknade, för vilka gäller att det i de lagar som nämns i 9 § för polisen har föreskrivits uppgifter relaterade till beviljande och tillsyn. Bestämmelser som preciserar de registerföringsskyldigheter som föreskrivits för polisen samt innehållet i registren ingår även i speciallagarna om polisens tillståndsförvaltningsuppgifter. Exempelvis i 42 b § (1184/2013) i lotterilagen föreskrivs det om tillsynsregister över lotterier, i 29 § i passlagen (671/2006) föreskrivs det om passregister och i 31 § i lagen om identitetskort (663/2016) föreskrivs det om identitetskortsregister.

I 2–5 mom. beaktas sådana personuppgifter inom särskilda kategorier av personuppgifter, uppgifter för identifiering av utlänningar och uppgifter om informationskälla och sådan säkerhetsinformation som polisen ska ha rätt att behandla för skötseln av de uppgifter som avses i 3–5 och 9 § i anknytning till det behandlade ärendet, polisens uppgifter, åtgärder eller händelser. I 2 mom. föreskrivs om polisens rätt att behandla särskilda kategorier av personuppgifter, nämligen biometriska och genetiska uppgifter samt andra kategorier av personuppgifter enligt artikel 9 i dataskyddsförordningen och 11 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I EU:s dataskyddslagstiftning har behandlingen av dessa kategorier av personuppgifter bundits vid en högre behandlingströskel än behandlingen av andra personuppgifter. Bestämmelsen täcker polisens rätt att behandla särskilda kategorier av personuppgifter i brottmål för att fastställa identiteten eller registrera gärningsmän, signalement som avses i tvångsmedelslagen samt känsliga personuppgifter för de ändamål med behandlingen som anges i 9 §.

I fråga om de ändamål med behandlingen som anges i 3–5 § i kapitlet avses med biometriska och genetiska uppgifter följande uppgifter som för närvarande registreras i informationssystemet för polisärenden: 1) uppgifter om efterlysningar av personer, såsom fotografi, fingeravtryck samt särskilda oföränderliga fysiska kännetecken för att exempelvis efterlysta personer, personer som har meddelats nationellt inreseförbud, personer som försatts i övervakad frihet på prov eller personer som ett besöksförbud avses skydda ska kunna påträffas, övervakas, observeras och skyddas, 2) identifieringsuppgifter, såsom fotografier, fingeravtryck, tandkartor och DNA-profiler för att personer som anmälts försvunna ska kunna hittas och för att okända avlidna ska kunna identifieras, samt 3) signalementsuppgifter, såsom fotografier, finger-, hand- och fotavtryck samt handstils-, röst- och luktprov och DNA-profiler för identifiering av personer som misstänks för brott, för utredning av brott och för registrering av gärningsmän. På så sätt säkerställs att tvångsmedelslagen problemfritt kan tillämpas på behandlingen av personuppgifter. Det högre behandlingskriteriet för personuppgifter som avses i momentet bör beaktas även när fingeravtryck eller DNA-avtryck behandlas i system som möjliggör omfattande behandling av personuppgifter och som kan vara förenade med en annan EU-medlemsstats rätt att söka träffar i polisens informationssystem och på motsvarande sätt med polisens rätt att söka träffar i en annan medlemsstats system. Fingeravtrycks- och DNA-system som införts för att tillämpa Prümbesluten är exempel på sådana system.

I dataskyddsdirektivet fästs särskild uppmärksamhet vid behovet att begränsa sådan behandling av genetiska personuppgifter (skäl 23 i ingressen) som kan avslöja känslig information om bland annat personens hälsotillstånd. DNA-avtryck är dock väsentliga signalementsuppgifter för polisen vid utredning av brott, och med hjälp av dem kan en person identifieras på ett tillförlitligt sätt exempelvis när det inte finns några fingeravtryck. Även mellan de brottsbekämpande myndigheterna i EU-medlemsstaterna sker ett utbyte av DNA-uppgifter med hjälp av sökningar som gett träffar, och då handlar det om omfattande behandling av personuppgifter. I fråga om genetiska personuppgifter, liksom även i fråga om andra känsliga personuppgifter, bör det noteras att redan en sökning för träffar bland referensuppgifter inskränker integritetsskyddet för den berörda registrerade personen och kan försvaga hans eller hennes

ställning. Grundlagsutskottet har dock ansett att sökningar för träffar bland referensuppgifter är oproblematiska med tanke på grundlagen.

De biometriska och genetiska uppgifter som avses i 2 mom. omfattar även följande uppgifter som för närvarande registreras i informationssystemet för förvaltningsärenden: 1) bilduppgifter, det vill säga ett fotografi och namnteckningsprov för identifiering av en person och för utarbetande av en handling som styrker identiteten, samt 2) fingeravtrycksuppgifter i pass för skötseln av polisens, utrikesministeriets och finska beskickningars uppgifter enligt passlagen (761/2006). Polisen ska alltjämt med den berörda personens samtycke få behandla fingeravtrycksuppgifter i pass även för utarbetande av en identitetshandling som personen ansökt om senare. Även fotografiet och namnteckningsprovet ska med personens samtycke få användas också för något annat förvaltningstillstånd eller beslut som personen ansökt om än för den handling som fotografiet och namnteckningsprovet har lämnats för.

Biometriska uppgifter som behandlas för tillståndsförvaltningsändamål enligt den föreslagna 9 § i kapitlet samt uppgifter om hälsotillstånd som behövs för utredning av förutsättningarna för beviljande av ett tillstånd eller tillståndets giltighet ingår i de särskilda kategorier av personuppgifter som avses i artikel 9 i dataskyddsförordningen. Behandlingen av särskilda kategorier av personuppgifter för tillståndsförvaltningsändamål bygger på artikel 9.2 g, enligt vilken särskilda kategorier av personuppgifter får behandlas när behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Regleringen ska också stå i proportion till det eftersträvade syftet, vara förenlig 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. Sådana lämpliga och särskilda åtgärder utgörs förutom av skyddsåtgärderna enligt dataskyddsförordningen och den nationella dataskyddslagen också av bland annat de kriterier för behandlingen av personuppgifter som föreslås i 2 kap. 3–5 och 9 § och de förutsättningar för förenlig behandling som föreslås i 11 §, de förutsättningar för utlämnande av uppgifter som föreslås i 4 kap., de tider för bevarande som föreslås i 5 kap. 4 § samt den skyldighet att sörja för dataskyddet av känsliga uppgifter som föreslås för den personuppgiftsansvarige i 8 kap. 1 §. Som en skyddsåtgärd kan också anses speciallagstiftningen om tillståndsförvaltningsuppgifter, där det föreskrivs om ändamålen med behandlingen av personuppgifter samt om innehållet i olika register.

I 3 mom. föreskrivs det särskilt om polisens rätt att behandla uppgifter för identifiering av utlänningar, det vill säga i 131 § i utlänningslagen (301/2004) avsedda fingeravtryck, fotografier och andra signalement på en utlänning. Identifieringsuppgifterna ska få behandlas för skötseln av de uppgifter som föreskrivs för polisen i 131 § i utlänningslagen, nämligen för verifiering av identitet, för behandling, beslut och övervakning av utlänningars inresa och utresa samt vistelse och arbete och för tryggande av statens säkerhet. I 131 § i utlänningslagen ingår också en förteckning över de persongrupper vilkas identifieringsuppgifter får behandlas för skötseln av de nämnda uppgifterna. I gällande lag föreskrivs det om uppgifter för identifiering av utlänningar i samband med informationssystemet för förvaltningsärenden. De uppgifter som föreskrivs för polisen i 131 § i utlänningslagen kan dock inte jämställas med de tillståndsförvaltningsuppgifter och relaterade tillsynsuppgifter som avses i 2 kap. 9 § i lagförslaget. Identifieringsuppgifterna behandlas som ett led i den tillsynsuppgift som föreskrivs särskilt för polisen i utlänningslagen, nämligen övervakning av utlänningar som polisen utövar antingen som en separat åtgärd eller som en del av polisens övriga verksamhet, såsom trafikövervakning, brottsutredning, larmuppdrag eller i samband med uppgifter med anknytning till allmän ordning och säkerhet (RP 169/2014 rd, s. 23).

I 4 mom. föreslås en bestämmelse om behandling av uppgifter om informationskälla. Det handlar om en persongrupp vars personuppgifter på grund av sakens känsliga natur eller för att

skydda personen, så långt det är möjligt ska åtskiljas från andra personuppgifter som har samband med brottsmisstanke. Polisen ska få behandla de uppgifter som avses i momentet när det handlar om uppgifter om en i 5 kap. 40 § i polislagen eller 10 kap. 39 § i tvångsmedelslagen avsedd person som har använts för de ändamål som anges i 3 och 4 §, inklusive specificerade uppgifter om hur informationskällan har använts och om tillsynen samt det huvudsakliga innehållet i de uppgifter som informationskällan lämnat. Syftet med bestämmelsen motsvarar syftet med 2 § 3 mom. 9 punkten i den gällande lagen, men för tydlighetens skull föreslås en hänvisning till tvångsmedelslagen bli fogad till bestämmelsen. Bestämmelser om registrering av informationskällor finns dessutom i 3 kap. 13 § 2 mom. och 14 § i statsrådets förordning om förundersökning, tvångsmedel och hemligt inhämtande av information (122/2014).

I 5 mom. föreslås en bestämmelse om behandling av så kallad säkerhetsinformation. Momentet preciserar bestämmelsen om behandling av känsliga personuppgifter för att beakta att de bör kunna kombineras med övriga uppgifter som rör en person som bedömts vara farlig eller oberäknelig och vilka i synnerhet beskriver eller är avsedda att beskriva en brottslig gärning, ett straff eller någon annan påföljd för brott. Bestämmelsen medför inte behörighet att lämna ut personuppgifter av detta slag, utan avsikten är att göra det möjligt för polisen att behandla även känsliga personuppgifter för att få en helhetsbild av om personen i fråga utgör en brottsrisk eller är en risk för sin egen säkerhet eller för en myndighets säkerhet i arbetet, med beaktande av personens eventuella tidigare brott. Bestämmelsen motsvarar 2 § 3 mom. 6 punkten i den gällande lagen.

3 §. *Behandling av personuppgifter i utredningssyfte.* I paragrafen avses behandling av personuppgifter för förebyggande, utredning eller avslöjande av brott i enlighet med dataskyddsdirektivet och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Bestämmelsen täcker alla former av undersökning och utredning som polisen utför, inklusive utredning som föregår förundersökning samt polisundersökning som anknyter till olika ärenden. Även teknisk undersökning som ingår i förundersökning eller polisundersökning omfattas av bestämmelsens tillämpningsområde. Bestämmelsen ersätter de bestämmelser i den gällande lagen som gäller registrering i informationssystemet för polisärenden av uppgifter som gäller identiteten i fråga om den som är misstänkt för brott eller den som är föremål för förundersökning, polisundersökning, polisens åtgärder eller tvångsmedel och den som gjort anmälan, den som uppträder som vittne eller målsägande eller den som har något annat samband med ärendet. På sådan behandling av personuppgifter som avses i 1 mom. ska till alla delar lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten tillämpas.

I 2 mom. preciseras de persongrupper vilkas uppgifter i tillämpliga delar ska få behandlas i utredningssyfte. I förteckningen avses i huvudsak personer som har samband med det behandlade brottmålet. Minderåriga personer som gjort sig skyldiga till en brottslig gärning beaktas särskilt. Den som har något annat samband med ärendet kan vara framför allt någon annan som har anmält ett brott än målsäganden eller offret samt en person som eventuellt ger ytterligare information men som inte har ställning som vittne. De som har något annat samband med ärendet omfattar även personer som har samband med någon annan undersökning än förundersökning. Genom 3 mom. genomförs som en komplettering av lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten artikel 6 i dataskyddsdirektivet, där det förutsätts att det i tillämpliga fall och så långt det är möjligt görs en klar åtskillnad mellan uppgifter som rör personer som tillhör olika kategorier. Behandling av personuppgifter i utredningssyfte kan också anknyta till sådan behandling av personuppgifter för upprätthållande av allmän ordning och säkerhet som avses i 5 § och där de situationer av skydd mot och förebyggande av hot mot den allmänna säkerheten som avses i skäl 12 i ingressen till dataskyddsdirektivet föreslås bli beaktade.

4 §. *Behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning.* Den föreslagna paragrafen är ny i förhållande till den gällande lagen. Till skillnad från den behandling av personuppgifter som avses i 3 § handlar 4 § inte om utredningsåtgärder, utan om behandling av personuppgifter som anknyter till olika åtgärder för kriminalunderrättelseinhämtning. Paragrafen ersätter den gällande lagens bestämmelser om informationssystemet för misstänkta, och dessutom kompletteras regleringen framför allt för att beakta kriminalunderrättelseinhämtningens karaktär vid behandling av personuppgifter. Uttrycket ”personuppgifter som anknyter till kriminalunderrättelseinhämtning” är ett paraplybegrepp, som kan inbegripa även exempelvis uppgifter som fåtts genom observation och iakttagande.

I likhet med 3 § gäller att i den behandling av personuppgifter som omfattas av paragrafens tillämpningsområde ingår sådan behandling av personuppgifter för att förebygga, utreda eller avslöja brott som omfattas av dataskyddsdirektivets tillämpningsområde. I skäl 27 i ingressen till dataskyddsdirektivet påpekas att om behöriga myndigheter ska kunna förebygga, förhindra, utreda och lagföra brott är det nödvändigt att de behandlar personuppgifter som insamlats inom ramen för förebyggande, förhindrande, utredning och lagföring av specifika brott i ett bredare sammanhang för att utveckla förståelsen för kriminell verksamhet och göra kopplingar mellan olika upptäckta brott. Också när det gäller personuppgifter som behandlas i kriminalunderrättelsesyfte bör det dock tas hänsyn till principen om ändamålsbundenhet samt de övriga krav som direktivet ställer på lagenlig och proportionerlig behandling och om vilka det föreskrivs i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Begreppet kriminalunderrättelseinhämtning har inte definierats på lagstiftningsnivå. I regeringspropositionen om polisens tidigare personuppgiftslag hänvisas det till den administrativa föreskriften om polisens kriminalunderrättelseverksamhet (RP 93/2002 rd, s. 26–27). I föreskriften har det konstaterats att kriminalunderrättelseverksamheten och den brottsanalys som ansluter sig till den är planerad och organiserad informationshantering i syfte att uppnå de mål som nämns i 1 § i polislagen samt att stödja polisens strategiska beslut gällande bekämpningen av brott. Med hjälp av kriminalunderrättelseverksamhet inhämtas, analyseras och förmedlas information som är väsentlig ur brottsbekämpningssynvinkel samt produceras utredningar gällande brottslingar, brott, brottsligheten, fenomen som utgör fara för samhället samt de följder brottsligheten ger upphov till.

I det sammanhanget behandlas också begreppet observation utgående från bestämmelsen om detta i den tidigare polislagen och utgående från förarbetena till bestämmelsen. I förarbetena konstateras det att observation är det överordnade begreppet för de operativa metoder som står till förfogande. Dessa omfattar de metoder för inhämtande av information om vilka det föreskrivs i polis- och tvångsmedelslagen samt det styrda utnyttjandet av informatörer.

Eftersom både polislagen och tvångsmedelslagen ändrades betydligt genom de reformer som trädde i kraft 2014 (tvångsmedelslagen 806/2011, polislagen 872/2011) i synnerhet när det gäller hemliga metoder för inhämtande av information, kan användningen av begreppet observation i detta sammanhang förorsaka förvirring i fråga om bestämmelserna om systematisk observation, om vilken det föreskrivs på ett samstämmigt sätt i polislagen och tvångsmedelslagen. Vid ingången av 2014 trädde också en ändring (1181/2013) av polisväsendets personuppgiftslag i kraft genom vilken det föreskrevs särskilt om observationsuppgifter. I det sammanhanget avsågs uppgifter om observationer som gjorts av poliser eller uppgifter som anmälts till polisen i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser eller uppträdande i övrigt med fog kan bedömas ha samband med brottslig verksamhet. Avsikten är att bestämmelsen om observationsuppgifter ska kvarstå med nästan samma innehåll i 2 kap. 6 § i den nya lagen.

I paragrafen om kriminalunderrättelseuppgifter är det därför inte nödvändigt att göra åtskillnad mellan olika slag av uppgifter på basis av observation eller iakttagelser. Med anledning av den ändrade lagstiftningen bör kriminalunderrättelseinhämtning ses som ett överordnat begrepp som i princip omfattar alla metoder för informationsinhämtning som står till förfogande för polisen och alla uppgifter som på något annat sätt kommit till polisens kännedom och som kan bedömas ha betydelse för kriminalunderrättelseinhämtningen. Uppgifter som polisen fått i samband med polisens övriga uppdrag (exempelvis förundersökningsåtgärder, larmuppdrag, trafikövervakning) kan nämnas som exempel på uppgifter som polisen fått på något annat sätt än genom sina egentliga informationsinhämtningsmetoder. Det är också möjligt att information som har betydelse för kriminalunderrättelseinhämtningen fås ur offentliga källor, som har ökat i antal de senaste åren i och med olika internetbaserade kanaler.

Det gäller också att beakta att de begränsningar för att registrera eller använda information som erhållits med sådana hemliga informationsinhämtningsmetoder och tvångsmedel som nämns särskilt ska beaktas vid behandlingen av personuppgifter som anknyter till metoderna eller medlen. (Tvångsmedelslagen 806/2011, polislagen 872/2011)

I initialstadiet går det inte alltid att dra speciellt långtgående slutsatser om vilken betydelse personuppgifter som anknyter till kriminalunderrättelseinhämtning har, utan personuppgifternas betydelse kan konkretiseras först i ett senare skede exempelvis i och med kompletterande information. Tröskeln för att registrera personuppgifter föreslås därför vara rätt låg i fråga om 4 § i lagförslaget. Det här accentueras framför allt vid underrättelseinhämtning som gäller organiserad brottslighet. Bärande av yttre symboler, överlåtelse av fordon till förfogande för personer som tillhör organiserade kriminella sammanslutningar, misstankar om verksamhet som bulvan med eventuella skenrättshandlingar är typiska vid skapandet och upprätthållande av en lägesbild över organiserade brottslighet. Även tidigare brottslighet är en potentiell faktor som förutspår framtida brottslig verksamhet exempelvis för sådana personer som dömts för våld-, egendoms- eller narkotikabrott eller ekonomiska brott och som kan antas fortsätta med brottslig verksamhet när de blir frigivna. Här krävs det övergripande prövning från fall till fall.

Syftet med kriminalunderrättelseinhämtning är att identifiera sådant som reser sig ur så kallade tysta signaler samt att försöka förebygga att brottsliga handlingar begås och att stegrande fenomen förvärras till eventuella problem som hotar den allmänna ordningen och säkerheten. Skolskjutningar och den senaste tidens fenomen relaterade till radikalisering kan nämnas som de allvarligaste exemplen under de senaste åren. Kriminalunderrättelseinhämtning med tillhörande behandling av personuppgifter spelar en viktig roll när det gäller att bekämpa dessa och upptäcka tidiga tecken på dem. För behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning ska det därför inte krävas någon exakt specificering av ett eventuellt brott.

Kriminalunderrättelseinhämtning kan utföras inte bara för att utreda och avslöja brott utan också för att förebygga brott, och behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning kan således ha samband med den behandling av personuppgifter som anknyter till upprätthållandet av den allmänna ordningen och säkerheten samt den nationella säkerheten i enlighet med skäl 12 i ingressen till dataskyddsdirektivet.

De gällande bestämmelserna om informationssystemet för misstänkta har ansetts vara oklara framför allt i fråga om de persongrupper som bestämmelserna gäller. Den gällande paragrafen om ett register över misstänkta har ansetts vara oklar också när det gäller registreringens syfte och ändamålet med personuppgifterna och när det gäller i vilken utsträckning paragrafen möjliggör behandlingen av så kallade tips. Möjligheterna att dra nytta av registret har därför ansetts vara bristfälliga med hänsyn till förändringarna i den EU-lagstiftning och nationella lagstiftning som reglerar polisens verksamhet och med hänsyn till förändringarna i omvärlden.

Avsikten är att den föreslagna nya bestämmelsen ska göra det möjligt att genom behandling av personuppgifter möta behoven enligt moderna kriminalunderrättelsemetoder, dock så att särskild uppmärksamhet fästs vid ställningen och rättsskyddet för de persongrupper som avses i bestämmelsen.

I 1 mom. anges de ändamål som personuppgifter som anknyter till kriminalunderrättelseinhämtning huvudsakligen ska få användas för (ursprungliga ändamål med behandlingen). Sådana ändamål är enligt 1 punkten sådan kriminalunderrättelseinhämtning och brottsanalys som behövs för att förebygga, avslöja eller utreda brott på vilka det kan följa fängelse, samt för att utföra uppgifter i anknytning till kriminalunderrättelseinhämtningen och brottsanalysen, och enligt 2 punkten utarbetande av sådana strategiska och tematiska analyser som behövs för att utföra en uppgift. Syftet med momentet är också att möjliggöra övergripande analyser av exempelvis organiserad brottslighet och personer med kopplingar till sådan verksamhet eller enskilda personer som bedöms ha kopplingar till ett brott eller brottslig verksamhet, genom att genom en explicit bestämmelse tillåta behandling av personuppgifter i samband med analyser av detta slag. Med stöd av den gällande lagen utförs analyser i temporära enhetsvisa datafiler och register. Det föreslagna 1 mom. kompletteras av de bestämmelser om förenlig behandling som föreslås i 11 §.

I 2 mom. anges de persongrupper vilkas personuppgifter ska få behandlas i huvudsak för de ändamål med behandlingen som anges i 1 mom. Som behandlingströskel föreslås uttrycket ”kan antas”, som bättre beskriver den registreringströskel som behövs vid kriminalunderrättelseinhämtning och som ännu inte utgör tröskeln för att inleda förundersökning. Med uttrycket ”ha gjort sig skyldiga till brott” avses en situation där det har inkommit tips om att ett brott redan har begåtts men nivån för att inleda förundersökning, ”skäl att misstänka”, ännu inte har nåtts. Med uttrycket ”kan antas göra sig skyldiga” avses ett sådant planerat brott och ett sådant brott som håller på att begås som kriminalunderrättelseinhämtningen avses förhindra. I momentet avses personer för vilka det finns ett samband med den förmodade brottsliga verksamheten, men rollen för alla personer med anknytning till saken är inte nödvändigtvis klar. Den behandling av uppgifter om kriminalunderrättelseinhämtning, observationer och iakttagelser som avses i paragrafen ska dock kunna ha kopplingar till behandling av personuppgifter i utredningssyfte.

Den persongrupp som avses i 1 punkten omfattar förutom förmodade gärningsmän också medverkande enligt straffrättens medverkanslära, det vill säga medhjälpare, anstiftare och medgärningsmän. I 2 punkten avses personer som annars kan antas främja brott som avses i den punkten. Som exempel kan nämnas hyresvärdar som fullt medvetna om användningsändamålet har hyrt ut en bostads- eller kontorslägenhet för brottslig verksamhet.

I den nya lagen föreslås en bestämmelse om personer som har samband med ett brott, vilken kompletterar omnämnandet av medverkande och brottsfrämjande personer. I 2 mom. 3 punkten nämns personer som upprepat har kontakt med en i 1 eller 2 punkten avsedd person eller upprepat påträffas i dennes sällskap, och kontakten eller sammanträffandena antas ha samband med ett brott. Den kategori av registrerade som föreslås i punkten ingår inte i den gällande lagen. I artikel 6 i dataskyddsdirektivet finns bestämmelser om åtskillnad mellan olika kategorier av registrerade, och i led d i artikeln nämns personer med kontakter med eller band till personer som nämns tidigare i artikeln, nämligen personer avseende vilka det finns tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott och personer som dömts för brott. Begreppet definieras dock inte närmare i dataskyddsdirektivet, och i momentet föreslås därför ett närmare beaktande av olika persongrupper med kopplingar till förmodad brottslig verksamhet.

När det gäller personer som upprepat har kontakt med en person som gör sig skyldig till brott bedöms betydelsen redan när det vid brottsanalys hittas flera kontakter mellan personer där den ena är en person som avses i 1 punkten och den andra inte är en sådan person. Det kan finnas en naturlig förklaring till en sådan relation, exempelvis ett kundförhållande. I 3 punkten avses personer via vilka det går att få betydelsefull information om personer som avses i 1 punkten och information av betydelse för analysen. I bestämmelsen förutsätts dock att även denna persongrupp har samband med ett förmodat brott, med beaktande av kriminalunderrättelseinhämtningens eventuella konsekvenser för de berörda personernas ställning och rättsskydd. Enbart ett antagande eller upprepade kontakter är följaktligen inte nog för att registreringströskeln ska överskridas.

I 2 mom. 4 punkten hänvisas det till observation i enlighet med 5 kap. 13 § 1 mom. i polislagen och 10 kap. 12 § i tvångsmedelslagen. Även uppgifterna om personer som är föremål för sådan observation ska få behandlas i kriminalunderrättelsesyfte.

I 3 mom. föreskrivs det om sådana persongrupper där personens roll är tydlig. I bestämmelsen beaktas att dessa persongrupper inte egentligen är målpersoner för polisens kriminalunderrättelseinhämtning. Behandlingen av personuppgifter som rör dessa persongrupper ska inte få gå längre än vad som är nödvändigt för att målet ska nås, exempelvis för att förebygga ett brott. Med nödvändighetskriteriet avses här att uppgifterna om persongrupperna får behandlas snävare för det ändamål med behandlingen som anges i paragrafen eller bara för ett avgränsat ändamål. Persongrupperna utgörs av offer för ett brott eller personer som uppträder som målsägande, personer som anmält ett brott och vittnen till ett brott. Med vittnen avses inte här nödvändigtvis personer som redan har utsetts till vittnen i en straffprocess. Det uppställs särskilda skyddsgarantier för behandlingen av personuppgifterna. Behandlingen av uppgifterna om dessa persongrupper kan vara nödvändig exempelvis vid försök att förebygga ett brott som riktas mot ett vittne till eller en målsägande i ett brott som redan har begåtts, exempelvis vid hot där en planerad gärning riktas mot en specificerad person. Som exempel kan nämnas en planerad kidnappning eller en organiserad kriminell sammanslutnings hämndaktion mot en person i en annan kriminell sammanslutning.

I 4 mom. föreskrivs det om en skyldighet att i samband med registrering av uppgifter om kriminalunderrättelseinhämtning, observation och iakttagelser om möjligt infoga en bedömning av uppgiftslämnarens eller källans tillförlitlighet och uppgifternas riktighet. I praktiken handlar det om ett vedertaget förfarande, där polisen bedömer uppgifternas tillförlitlighet på en fyrgradig skala. Bestämmelsen beaktar kravet enligt artikel 7.1 i dataskyddsdirektivet att personuppgifter som grundar sig på fakta så långt det är möjligt ska åtskiljas från personuppgifter som grundar sig på personliga bedömningar, med hänsyn till att uppgifter som fåtts genom iakttagelserna kan vara obekräftade. Bestämmelsen stöder också kravet enligt artikel 7.2 att felaktiga, ofullständiga eller inaktuella personuppgifter inte får överföras eller göras tillgängliga. Polisen ska också i den mån det är praktiskt möjligt kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga.

Vid formuleringen av den föreslagna paragrafen har avseende fästs vid förvaltningsutskottets påpekanden om registret över misstänkta. I paragrafen föreslås en uttömmande förteckning över de persongrupper som i fråga om uppgifter om kriminalunderrättelseinhämtning ska få registreras i informationssystemet. Det uppställs särskilda registreringsrelaterade kriterier för införande i register och för annan behandling av personuppgifter som anknyter till dessa persongrupper. När det är fråga om andra än personer som antas ha kopplingar till egentlig brottslig verksamhet ska registrering vara möjligt, men behandling av personuppgifter är förenad med kravet att behandlingen ska vara nödvändig för utförandet av ett uppdrag. När det är fråga om personer som kan antas begå eller ha begått brott ska tröskeln för registrering i informationssystemet vara lägre än för de personer som avses ovan.

I 4 mom. i den gällande 4 §, som gäller registret över misstänkta, ingår en begränsande bestämmelse enligt vilken endast polispersonal som förordnats till kriminalunderrättelse-, brottsanalys- och observationsuppgifter samt de kontaktpersoner som polisen sänt utomlands har tillgång till informationssystemet för misstänkta genom teknisk anslutning. Den föreslagna paragrafen avser inte att utvidga denna personkrets. I 4 § i lagförslag 1 föreslås dock inte någon motsvarande begränsande bestämmelse, utan det bedöms att tillträdet till registret begränsas genom den allmänna regleringen av informationssäkerhet. Bestämmelser om informationssäkerhet föreslås i 32 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Enligt 5 punkten i den paragrafen ska den personuppgiftsansvarige säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras nyttjanderätt. Användarrättigheter till polisens informationssystem beviljas utifrån polisens arbetsuppgifter.

5 §. *Behandling av personuppgifter för upprätthållande av allmän ordning och säkerhet.* I paragrafen avses sådan behandling av personuppgifter i anknytning till polisens uppdrag som inte med säkerhet anknyter till ett sådant ändamål med behandlingen som föreskrivs i 3 och 4 § men som senare kan visa sig anknyta till ett brottmål. Avsikten är att paragrafen ska beakta situationer där polisen i praktiken kan ha svårt att avgöra om det är fråga om ett brottmål eller ett ärende som hänför sig till allmän ordning och säkerhet, och tillåta behandling av personuppgifter även i sådana situationer. Paragrafens tillämpningsområde omfattar framför allt personuppgifter som registreras i samband med polisens fältarbete och som larmuppgifter samt personuppgifter som tagits till vara i samband med övervakning och handräckning under stora idrottsevenemang eller andra evenemang för allmänheten eller demonstrationer eller upplopp. Även behandling av personuppgifter i gränsdragningsfall av detta slag är automatiskt sådan behandling av personuppgifter som omfattas av dataskyddsdirektivet när behandlingen utförs av en i direktivet avsedd behörig myndighet. I paragrafen är det fråga om sådan behandling av personuppgifter som omfattas av direktivets tillämpningsområde och som utförs för att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten.

6 §. *Behandling av observationsuppgifter.* Paragrafen kompletterar 3 och 4 § genom att den innehåller särskilda villkor för registrering av observationsuppgifter. Bestämmelsen motsvarar 2 § 2 mom. 11 punkten i den gällande lagen. Observationsuppgifterna kan innehålla uppgifter om observationer som gjorts av polismän eller uppgifter som anmälts till polisen i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser eller uppträdande i övrigt kan bedömas ha samband med brottslig verksamhet. Om observationsuppgifterna når över tröskeln för ett sådant ändamål med behandlingen som anges i 3 eller 4 §, kan uppgifterna kopplas samman med ändamålet. Det är fråga om uppgifter som polisen får genom att iaktta sin omvärld eller uppgifter som en utomstående har meddelat polisen. Polisen kan få exempelvis ett anonymt tips om personer som beter sig tvivelaktigt eller om tvivelaktig verksamhet som inte i och för sig nödvändigtvis är lagstridig verksamhet. I kombination med andra faktorer eller i kombination med förhållandena kan observationsuppgifterna dock ge fingervisningar om brottslig verksamhet. Polisen får också observationsuppgifter från utomstående, exempelvis via systemet för nättips. Av de inkomna tipsen förmedlas vissa vidare till polisenheterna för fortsatta åtgärder, nämligen sådana tips där man måste överväga om det rör sig om någonting sådant som bör skötas av polisen eller om det finns skäl att misstänka brott. Genom att analysera uppgifterna försöker man förhindra, avslöja och utreda brott och brottsplaner, identifiera gärningsmännen och mot gärningsmännen rikta in eventuella åtgärder för övervakning av tillstånd som stöder förhindrandet av brott.

Vidare föreslås det att ett uttryckligt krav på bedömning av uppgifternas tillförlitlighet och riktighet fogas till paragrafen. När det gäller observationsuppgifter har grundlagsutskottet (GrUU 18/2012 rd) konstaterat att det handlar om en potentiellt mycket omfattande datamängd som berör privatlivet. Observationsuppgifter är dessutom ofta av otillförlitligt slag och det finns

risk för att oskyldiga personer stämplas. Grundlagsutskottet har tidigare utöver de ovan relaterade allmänna iakttagelserna påpekat vikten av att försäkra sig om observationsuppgifters korrekthet och tillförlitlighet (GrUU 27/2006 rd, s. 2) och behovet att komplettera uppgifterna med en bedömning av uppgiftslämnarens tillförlitlighet och uppgifternas riktighet (GrUU 51/2002 rd, s. 2).

7 §. *Behandling av uppgifter som inte hänför sig till ett visst uppdrag.* I 1 mom. avses behandling av sådana uppgifter som inte hänför sig till ett visst uppdrag men för vilka det redan när de erhålls är känt att polisen behöver dem för de ändamål med behandlingen som föreskrivs i 3–6 §. Paragrafen motsvarar i sak till övervägande del 12 § i polisens gällande personuppgiftslag. I motiveringen (RP 66/2012 rd, s. 24) till 2013 års lagändring har uppgifter som inte hänför sig till ett visst uppdrag definierats som information som polisen har kommit över i samband med utförandet av sina tjänsteuppdrag och som polisen kommer över i samband med andra uppdrag och som man inte skilt försöker inhämta. Polisen kommer emellertid över personuppgifter som inte hänför sig till ett visst pågående uppdrag men som är betydelsefulla för polisens uppgifter också när polisen inhämtar uppgifter i anslutning till ett specifikt uppdrag. Även sådana uppgifter ska få behandlas med stöd av det föreslagna momentet. De uppgifter som avses i momentet ska alltid ha inhämtats eller fåtts på något annat sätt med stöd av polisens lagstadgade befogenheter i samband med utförandet av polisens uppgifter. Bestämmelsen utvidgar således inte polisen befogenheter för informationsinhämtning, utan den uppställer specialvillkor för polisen när det gäller behandling av uppgifter som fåtts utifrån befogenheter som föreskrivs någon annanstans.

Enligt 12 § i den gällande lagen får uppgifter som inte hänför sig till ett visst uppdrag registreras i informationssystemet för polisärenden som observationsuppgifter, i informationssystemet för misstänkta, i skyddspolisens funktionella informationssystem och i det nationella systemet inom Schengens informationssystem. Till skillnad från den gällande lagen innebär den föreslagna bestämmelsen att uppgifterna får behandlas för alla ändamål som föreskrivs i 3–6 §, om behandlingen uppfyller de villkor som anges i paragraferna. I praktiken utvidgar den föreslagna ändringen inte de tillåtna ändamålen med behandlingen, eftersom det alltid krävs att de kriterier för behandlingen som föreskrivs i 3–6 § är uppfyllda. Observationsuppgifter får också enligt den gällande lagen överföras till andra delar i informationssystemet för polisärenden, förutsatt att registreringskriterierna är uppfyllda.

De uppgifter som avses i det föreslagna 1 mom. omfattar inte överskottsinformation som fåtts genom polislagens hemliga metoder för inhämtande av information. Bestämmelser om behandling av sådan överskottsinformation föreslås i 8 §.

Bestämmelserna i 2 mom. är nya. Även i 2 mom. handlar det om att information som inhämtats i samband med polisuppdrag och erhållits på något annat sätt behandlas i situationer där informationen inte hänför sig direkt till ett visst aktuellt uppdrag. Ett syfte är att skapa större klarhet i nuläget i fråga om situationer där personuppgifter som fåtts i samband med polisuppdrag ska behandlas med hjälp av automatisk databehandling för bedömning av innehållet och relevansen. Skäl 18 i ingressen till dataskyddsdirektivet har relevans för det föreslagna momentet. I skälet sägs att för att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Begreppet automatiserad behandling av personuppgifter omfattar således förutom registrering, användning av registeruppgifter och utlämnande av registeruppgifter också de behandlingsåtgärder som utförs innan uppgifterna registreras i polisens riksomfattande informationssystem. Denna fas i behandlingen av personuppgifter börjar omfattas av reglering på lagnivå genom det föreslagna 2 mom., där det föreskrivs att innan uppgifter registreras för

en längre tid i polisens informationssystem ska det bedömas om uppgifterna behövs. Till denna del utvidgas regleringen i jämförelse med polisens gällande personuppgiftslag. Den gällande regleringen gäller registrering och behandling av uppgifter i polisens riksomfattande och enhetsvisa informationssystem.

Förutom att 2 mom. förtydligar nuläget innebär det också att polisens nuvarande behandling av personuppgifter breddas. Till skillnad från den gällande lagen möjliggör momentet registrering av personuppgifter i ett separat personregister för att det ska kunna klarläggas om de villkor för behandling av uppgifterna som anges i 3–6 § är uppfyllda. Personuppgifter ska inte få behandlas i utrednings- eller underrättelseinhämtningssyfte, för upprätthållande av allmän ordning och säkerhet eller som observationsuppgifter, om det är oklart huruvida de kriterier för behandling av personuppgifter som anges i 3–6 § är uppfyllda. Personuppgifter som fåtts i samband med polisuppdrag ska dock i högst sex månader få behandlas för bedömning av om de behövs, om uppgifterna kan ha betydelse med tanke på de syften som anges i 3–6 §. Personuppgifter som är klart onödiga med tanke på polisens uppgifter ska utplånas omedelbart, och uppgifterna ska inte kunna registreras med stöd av 2 mom.

Polisens omvärld har förändrats markant efter det att polisens gällande personuppgiftslag stiftades. Polisens traditionella sätt att bedöma uppgifternas relevans erbjuder inte tillräckliga möjligheter för att i en modern digital miljö behandla uppgifter som behövs vid brottsanalys. För att analysverksamheten ska kunna utvecklas på ett systematiskt sätt måste det vara möjligt att bedöma uppgifternas betydelse med moderna tekniska medel. De uppgifter som behandlas med stöd av det föreslagna momentet kan också bestå av bildmaterial och text från offentliga källor, såsom internet och myndigheternas offentliga register, och innehålla till och med stora mängder information om personer vars relevans är oklar när uppgifterna registreras. Med stöd av det föreslagna 2 mom. kan uppgifterna också jämföras med redan registrerade personuppgifter i polisens informationssystem för att klarlägga om de kriterier för behandling av uppgifterna som anges i 3–6 § är uppfyllda. För behandling förutsätts det dock i analogi med 1 mom. att uppgifterna har inhämtats eller fåtts på något annat sätt i samband med polisuppdrag med stöd av befogenheter från något annat ställe i lag. Med stöd av det föreslagna 2 mom. kan polisen således inte inhämta sådana uppgifter som polisen inte har tillgång till med stöd av informationsinhämtningsbefogenheter från något annat ställe i lag.

Dataskyddslagstiftningen förutsätter att personuppgifter inte behandlas i onödan. I 2 mom. föreskrivs det om hur det i fråga uppgifter som fåtts i samband med uppdrag kan bedömas om uppgifterna behövs och säkerställas att de är relevanta innan de behandlas i utrednings- eller kriminalunderrättelsesyfte, för ändamål som hänför sig till upprätthållande av allmän ordning och säkerhet eller som observationsuppgifter. I den sista meningen i momentet understryks det krav som anges i 6 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, nämligen att onödiga uppgifter ska raderas utan onödigt dröjsmål. Kravet kompletteras av den tidsgräns på sex månader som föreslås bland utplåningsbestämmelserna i 5 kap. 3 §. Senast inom den tiden ska det bedömas om personuppgifterna är betydelsefulla eller onödiga.

Registrering av uppgifter innan det har säkerställts att de behövs är en åtgärd som inskränker integritetsskyddet. I registret införs då oundvikligen också uppgifter som vid en bedömning av om de behövs visar sig vara betydelselösa med tanke på polisens uppgifter. De registrerades rättssäkerhet främjas dock av att uppgifterna ska få bevaras i högst sex månader och att uppgifter som bedömts vara onödiga ska utplånas utan dröjsmål redan innan det har gått sex månader. En skyddsåtgärd som garanterar att integritetsskyddet tillgodoses är också att uppgifterna ska få behandlas endast på beslut av en polisman som hör till befälet. Via kontrollen av polisens användarrättigheter begränsas tillgången till information till att gälla enbart för de personer i vilkas uppgifter det ingår att utföra den bedömning av betydelsefullheten som avses

i momentet. På motsvarande sätt som för andra ändamål med behandlingen gäller för behandlingen av uppgifterna att den omfattas av de skyldigheter som hänför sig till styrning av och tillsyn över samt skydd för uppgifterna vid behandling av personuppgifter. Behandlingen omfattas av alla de skyldigheter som i lagen föreskrivs för den personuppgiftsansvarige, såsom skyldigheten enligt 8 kap. 1 § att säkerställa skyddet av känsliga uppgifter till den del det material som ska behandlas innehåller känsliga uppgifter. Den registrerade ska inte ha rätt till insyn i de uppgifter som avses i det föreslagna 2 mom., men den registrerade ska ha rätt att be dataskyddsmyndigheten kontrollera lagenligheten i behandlingen av uppgifterna på det sätt som föreskrivs i 6 kap. 2 § 3 mom. i lagförslaget.

8 §. *Behandling av överskottsinformation som erhållits med hemliga informationsinhämtningsmetoder.* I paragrafen föreskrivs det om behandling av överskottsinformation som fåtts i samband med användning av hemliga metoder för inhämtande av information. Innehållet i paragrafen motsvarar 11 § i den gällande lagen. Bestämmelser om förutsättningarna för att lagra överskottsinformation finns i 10 kap. 57 § i tvångsmedelslagen (806/2011) och i 5 kap. 55 § i polislagen (872/2011). När förvaltningsutskottet bedömde den lagändring som trädde i kraft 2014 förutsatte det (FvUB 6/2013 rd, s. 7) att de förutsättningar för lagring som anges i polislagen och tvångsmedelslagen kompletteras i polisväsendets personuppgiftslag genom att det anges i vilka informationssystem eller personregister överskottsinformationen ska lagras. I lagförslag 1 föreskrivs det inte längre om informationssystem eller personregister, och därför föreslås det att den gällande regleringen enligt 11 § om registrering av överskottsinformation i de informationssystem som avses i 2, 4 och 5 § i den gällande lagen eller i det personregister som avses i 6 § 2 mom. 2 punkten i den gällande lagen ändras så att det föreskrivs att informationen får registreras för sådana ändamål med behandlingen av personuppgifter som föreskrivs i 2 kap. 3 och 4 §. Hänvisningen till behandlingen av skyddspolisens personuppgifter slopas.

I 2 mom. föreslås i analogi med gällande 11 § en informativ hänvisning till 5 kap. 54 § i polislagen och 10 kap. 56 i tvångsmedelslagen, där det föreskrivs om användning av överskottsinformation som fåtts genom teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter och teknisk observation.

9 §. *Behandling av personuppgifter i tillståndsförvaltnings- och tillsynsuppgifter samt i uppgifter enligt hittegodslagen.* Den behandling av personuppgifter som genomförs för att de uppgifter som avses i paragrafen ska kunna utföras omfattas av tillämpningsområdet för dataskyddsförordningen och den nationella dataskyddslag som kompletterar förordningen. Paragrafen ersätter de bestämmelser i 3 § i den gällande lagen som gäller uppgifter som ska registreras i informationssystemet för förvaltningsärenden, bortsett från de uppgifter för identifiering av utlänningar som avses i 3 § 2 mom. 7 punkten. En bestämmelse om behandlingen av dessa uppgifter föreslås i 2 §. Uppgifter för identifiering av utlänningar ska få behandlas för utförande av uppgifter som omfattas av tillämpningsområdet för lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

I 1 mom. föreslås en uttömmande förteckning över de författningar som omfattas av dataskyddsförordningens tillämpningsområde och där det föreskrivs om polisens tillståndsförvaltnings- och tillsynsuppgifter samt uppgifter inom hittegodsverksamheten. Utförandet av uppgifterna enligt de lagar som nämns i förteckningen utgör det ursprungliga ändamålet med behandlingen av personuppgifter enligt 9 §. Till gruppen av lagar fogas till skillnad från 3 § i den gällande lagen hittegodslagen (778/1988), lagen om skjutbanor (763/2015) och lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017). I polisens gällande personuppgiftslag finns inga bestämmelser om behandling av personuppgifter som behövs för utförandet av uppgifter som föreskrivs i dessa lagar. Paragrafen ska tillämpas tillsammans med dataskyddsförordningen och den dataskyddslag som kompletterar förordningen.

Personuppgifter som behandlas inom hittegodsverksamheten överförs med stöd av det föreslagna tillägget till polisens riksomfattande registerföring från de enhetsvisa personregister som inrättats med stöd av 6 § i den gällande lagen och där uppgifterna hittills har registrerats. När de tillståndsförvaltningsuppgifter som föreskrivs för polisen i lagen om skjutbanor fogas till ändamålen med behandlingen blir det möjligt att i polisens informationssystem behandla även personuppgifter som anknyter till de uppgifterna. Den tillståndsprövning som föreskrivs som polisens uppgift i lagen om skjutbanor förutsätter också att personuppgifter behandlas för att utreda sökandens tillförlitlighet och lämplighet, och en bestämmelse om detta föreslås i 11 § 7 punkten. Den paragrafen gäller förenlig behandling.

I 2 mom. föreslås en förteckning över de persongrupper för vilka gäller att sådana personuppgifter enligt 1 och 2 § som anknyter till personer inom grupperna ska få behandlas för det ändamål som anges i den aktuella paragrafen. De persongrupper som avses i 1 punkten omfattar alla som ansöker om och beviljas tillstånd och godkännanden enligt de lagar som preciseras i 1 mom. samt anmälare, inklusive sökande och innehavare av pass och identitetskort. Den föreslagna 2 punkten täcker på motsvarande sätt utöver de persongrupper som nämns särskilt i punkten även bland annat sådana uppgifter om ombud för sammanslutningar och medlemmar i sammanslutningars förvaltningsorgan samt uppgifter om banansvariga enligt lagen om skjutbanor som behandlas för utförande av tillståndsförvaltningsuppgifter. De i 3 punkten avsedda personer som anknyter till en skjutvapenanmälan omfattar både de personer som är föremål för anmälan och de yrkesutbildade personer inom hälso- och sjukvården som gjort anmälan.

I 4 punkten föreskrivs det särskilt om behandling av personuppgifter som rör kontakt- eller ansvarspersoner för penninginsamlingar eller lotterier eller genomför sådana i praktiken. De personer som avses i punkten är inte sökande eller tillståndshavare och ingår således inte i de persongrupper som avses i 1 punkten.

I 5 punkten föreskrivs det om behandling av uppgifter om personer som är anställda hos ett penningspelsbolag eller en annan näringsidkare eller sammanslutning som i enlighet med bestämmelserna i lotterilagen eller lagen om förhindrande av penningtvätt och av finansiering av terrorism ska övervakas av polisen. Andra näringsidkare eller sammanslutningar omfattar i 3 kap. i lotterilagen och 2 kap. 2 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism avsedda näringsidkare och sammanslutningar som förmedlar deltagaranmälningar och deltagaravgifter i anslutning till penningspelssammanslutningars penningspel. Uppgifter om persongrupper som avses i punkten ska behandlas bland annat för handläggning av ärenden som hänför sig till tillsyn enligt 7 kap. i lagen om förhindrande av penningtvätt och av finansiering av terrorism och till administrativa påföljder enligt 8 kap. i den lagen.

Enligt 7 kap. 9 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism ska tillsynsmyndigheten förvalta ett system för att ta emot rapporter om misstänkta överträdelser av bestämmelserna i den lagen. I den föreslagna 6 punkten föreskrivs det därför särskilt om behandling av personuppgifter om personer som är rapportörer eller föremål för rapporter i enlighet med 7 kap. 9 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism.

Den föreslagna 7 punkten täcker andra persongrupper som ska behandlas för utförande av de tillståndsförvaltnings- och tillsynsuppgifter som föreskrivits för polisen samt för utförande av uppgifter inom hittegodsverksamheten, såsom personer i anslutning till expedieringsuppgifterna om handlingar, ett konkurs- eller dödsbos förvaltare och delägare i ett dödsbo, de som lämnar utlåtanden, personer som registreras utifrån hittegodslagen, sysslomän som förordnats enligt lagen om penninginsamlingar och lotterilagen samt fotografer som lagrar fotografier för tillståndshandlingar. Punkten omfattar även överlåtare av skjutvapen eller andra föremål som registrerats utifrån skjutvapenlagen samt vapenägare vilkas uppgifter registreras i vapenregis-

tersystemet för att möjliggöra den uppföljning av vapnens livscykel som vapenlagstiftningen förutsätter. I 7 punkten avsedda personer omfattar även andra personer med anknytning till polisens tillsynsuppgifter enligt de lagar som nämns i 1 mom. och vilkas personuppgifter behöver behandlas för utförandet av tillsynsuppdrag.

Som en del av den tillsyn över penningspelsbolag som nämns i 11 § i lotterilagen (1047/2001) behandlar polisen också sådana personuppgifter för bolagets kunder som ingår i kundregistret och spelmaterialet. Det föreslås ett separat 3 mom. för behandlingen av dessa personuppgifter. Behandlingen av penningspelsbolagens kund- och spelaruppgifter ska begränsas till sådan behandling som är nödvändig för utförandet av tillsynen, eftersom det ursprungliga ändamålet med behandlingen av personuppgifterna är behandling av penningspelsbolagets kunduppgifter. Polisen ska få behandla spelaruppgifter också för tillsyn enligt lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017), vilken riktas till penningspelssammanslutningar och näringsidkare och sammanslutningar som förmedlar deltagaranmälningar och deltagaravgifter i anslutning till penningspel, exempelvis för att klarlägga om ett penningspelsbolag eller dess ombud har identifierat kunden på det sätt som lagen kräver. Kundernas personuppgifter behövs dessutom för den verifiering av speltransaktioner som görs för att garantera spelarnas rättsskydd. När det gäller spelaruppgifter ska polisen få behandla framför allt följande personuppgifter: spelaridentifikation, födelsedatum, kön, kontaktuppgifter, dödsdatum, kundnummer som tilldelats av spelbolaget, spelarens kontonummer, registreringsdatum, spelkontots stängningsdatum, de spelgränser som spelaren uppställt, penningtransaktioner till spelkontot, uppgifter om speltransaktioner, spelspärrar och spelförbud. Förteckningen är inte uttömmande. En del av de uppgifter som behandlas kan direkt kopplas till en enskild spelare (exempelvis spelaridentifikation eller spelarens kontonummer) och personen kan följaktligen identifieras på basis av den informationen. En del av de uppgifter som behandlas är däremot sådana uppgifter med anknytning till personuppgifter (exempelvis spelgränser, spelspärrar och spelförbud) utifrån vilka en enskild spelare inte direkt kan identifieras, utan för identifiering krävs det att någon annan unik information om personen kopplas samman med den aktuella informationen. Uppgifter om spelare ska dock inte kunna kopplas samman med en enskild fysisk person enbart på basis av uppgifter som ett spelbolag överfört till polisen som en datamängd, utan polisen ska endast via spelbolaget kunna få uppgifter om en enskild spelares identitet.

10 §. *Behandling av personuppgifter som fåtts vid teknisk övervakning.* För teknisk övervakning som är ändamålsenlig för den operativa verksamheten krävs behörighet dels att utföra själva övervakningen, dels att behandla den information som fåtts genom övervakningen. Allmän behörighet för polisen att företa teknisk övervakning anges i 4 kap. 1 § i polislagen. Med teknisk övervakning avses enligt den paragrafen fortlöpande eller upprepat iakttagande eller fortlöpande eller upprepad avlyssning av fordon, fordonsförare, fotgängare eller allmänheten med hjälp av en teknisk anordning samt automatisk upptagning av ljud eller bild. Efter att på förhand ha informerat om saken får polisen företa teknisk övervakning på allmän plats eller väg, för upprätthållande av allmän ordning och säkerhet, förebyggande av brott, identifiering av personer som är misstänkta för brott samt för bevakning av särskilda övervakningsobjekt. I polisens gällande personuppgiftslag finns inte några bestämmelser om behandling av personuppgifter som fås vid teknisk övervakning. Syftet med den föreslagna 10 § är att möjliggöra sådan behandling av personuppgifter som har anknytning till sådan teknisk övervakning som avses i 4 kap. 1 § i polislagen.

11 §. *Förenlig behandling.* EU:s nya dataskyddslagstiftning förutsätter att personuppgifter i huvudsak behandlas bara för det i lag föreskrivna ändamål som de har insamlats för. Principen ingår redan i den gällande personuppgiftslagen. Dataskyddslagstiftningen innebär dock att personuppgifter kan behandlas även för andra ändamål, om bestämmelser om detta utfärdas genom lag och behandlingen behövs och står i proportion till det eftersträvade syftet. Med

hänsyn till grundlagsutskottets tolkningspraxis bör regleringen också vara tillräckligt detaljerad och noggrant avgränsad.

I dataskyddsdirektivet har principen om förenlig behandling av personuppgifter dock skärpts i viss mån i förhållande till den tidigare EU-regleringen, och även förenlig behandling av personuppgifter binds relativt starkt till direktivets tillämpningsområde. Detta ställer också speciella krav på utlämnandet av personuppgifter när det är fråga om andra myndigheter än behöriga myndigheter inom direktivets tillämpningsområde. Enligt skäl 29 i ingressen till direktivet bör personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål som omfattas av direktivets tillämpningsområde och bör personuppgifter inte behandlas för andra ändamål än att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av direktivet men som inte är det ändamål som uppgifterna insamlades för, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet.

Den föreslagna paragrafen om förenlig behandling av personuppgifter motsvarar i huvudsak 16 och 16 a § i den gällande lagen, men bestämmelserna utvidgas och preciseras till vissa delar. I den regeringsproposition som överlämnades 2012 föreslogs det att 16 § 2 mom. ändras så att användningen av uppgifter i informationssystemet för laglighetsövervakning uttryckligen ska nämnas. Det är viktigt att bestämmelsen kvarstår, också med beaktande av behoven att stärka en tillbörlig övervakning av polisens informationssystem.

I 1 mom. i den föreslagna paragrafen om förenlig behandling av personuppgifter föreslås en förteckning över de ändamål med behandlingen som anses vara sådana ändamål med behandlingen av personuppgifter som är förenliga med de ursprungliga ändamålen med behandlingen. Förteckningen är uttömmande, men punkterna möjliggör dock spelrum. Behandling av personuppgifter för att förebygga, avslöja eller utreda ett brott inrymmer också riktande av polisens verksamhet och upprätthållande av en lägesbild. De föreslagna bestämmelserna i 2 och 3 punkten är nya i jämförelse med 16 § 1 mom. i den gällande lagen, och till skillnad från tidigare innehåller 4 punkten också förhindrande av betydande miljö-, egendoms- eller förmögenhetsskada som en grund. Tillsynsuppgifter som rör penningspelsbolag och näringsidkare och sammanslutningar som är ombud för penningspelsbolag ska dock falla utanför momentet.

I 2 mom. beaktas genom en hänvisande bestämmelse dels sådana ändamål med behandlingen av personuppgifter som i dataskyddsdirektivet alltid ses som förenliga ändamål med behandlingen, dels med dessa jämförbara behov som polisen har att behandla personuppgifter för laglighetsövervakning och för analys-, planerings- och utvecklingsverksamhet. Personuppgifter ska också få användas för utbildningsverksamhet, om de är nödvändiga för att genomföra utbildningen. I dessa situationer handlar det inte om att utföra ett visst uppdrag, utan om ett generellare behov av att behandla personuppgifter för vissa ändamål. Innehållet i det föreslagna momentet motsvarar 16 § 2 mom. i den gällande lagen.

I 3 mom. föreskrivs det om en begränsning som gäller användningen av observationsuppgifter, uppgifter om kriminalunderrättelseinhämtning och personuppgifter som registrerats för bedömning av om uppgifterna behövs. Bestämmelsen innebär att uppgifterna inte får användas för att fatta beslut eller lämna utlåtande om beviljande av ett tillstånd eller tillståndets giltighet, när tillståndet enligt gällande bestämmelser är beroende av sökandens eller tillståndshavarens tillförlitlighet, lämplighet eller någon liknande egenskap, och det för bedömningen av egenskapen krävs uppgifter om sökandens eller tillståndshavarens hälsotillstånd, bruk av berusningsmedel, brottslighet eller våldsamma uppträdande. Avsikten är att beakta att observat-

ionsuppgifter och uppgifter om kriminalunderrättelseinhämtning ofta är overifierade, och i anslutning till detta att dessa uppgifter inte är föremål för annan än indirekt rätt till insyn via dataskyddsmyndigheten. Med tanke på personens rättsskydd är det viktigt att de personuppgifter som använts vid tillståndsprövning är exakta och korrekta. Begränsningen utgör dock inte något hinder för att observationsuppgifter och uppgifter om kriminalunderrättelseinhämtning används vid beslut om inledande av tillståndsförvaltningsåtgärder som hänför sig till redan beviljade tillstånd. Det handlar då om att rikta polisens verksamhet med stöd av 1 mom. 1 punkten.

I det föreslagna 3 mom. utesluts för tydlighetens skull även möjligheten att uppgifter som behandlas för att bedöma om de behövs används i samband med beslut eller utlåtande om beviljande av ett tillstånd eller tillståndets giltighet. Uppgifter som behandlas för att bedöma om de behövs kommer även i övrigt att omfattas av förenlig behandling först efter det att det har bedömts att uppgifterna behövs och de har överförts till sådana ändamål med behandlingen som avses i 3–6 §.

I 4 mom. föreskrivs det om en begränsning som gäller behandlingen av fingeravtrycksuppgifter om den som ansöker om pass. De ska få användas för andra ändamål än det ursprungliga ändamålet med behandlingen av uppgifterna endast om det är nödvändigt för att identifiera ett offer för en naturkatastrof, storolycka eller någon annan katastrof eller ett brott eller ett offer som annars förblivit oidentifierat. Grundlagsutskottet bedömde i sitt utlåtande 47/2010 rd att det att fingeravtrycksuppgifter i passregistret får användas för att identifiera ett offer som annars inte kan identifieras kan ses som ett sådant exakt avgränsat och obetydligt undantag från ändamålsbundenheten som utskottet krävt. Med oidentifierade offer avses i 4 mom. förutom avlidna också offer som svävar i allvarlig fara för sitt liv och sin hälsa och som exempelvis på grund av utdragen medvetslöshet kan identifieras endast med hjälp av fingeravtrycksuppgifter. Till den del det handlar om behandling av fingeravtrycksuppgifter i pass motsvarar innehållet i det föreslagna momentet 16 a § 1 mom. i den gällande lagen.

Det föreslagna 5 mom. är nytt i förhållande till den gällande lagen. Enligt gällande 16 a § 1 mom. får fingeravtrycksuppgifter som med stöd av 131 § i utlänningslagen registrerats i polisens register användas för andra ändamål än det ursprungliga ändamålet med behandlingen under samma förutsättningar som fingeravtrycksuppgifter i pass. Det föreslås att användningen av fingeravtryck som registrerats med stöd av utlänningslagen ska utvidgas så att fingeravtryck också får användas för förebyggande, avslöjande eller utredning av sådana terroristbrott och andra grova brott som avses i Europaparlamentets och rådets förordning (EU) nr 603/2013 (Eurodacförordningen). En förutsättning för användningen av fingeravtryck är i enlighet med 11 § 2 mom. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten att behandlingen är nödvändig. Dessutom ska jämförelsen begränsas till motsvarande brott som vid jämförelse av fingeravtryck enligt Eurodacförordningen. En förutsättning för att fingeravtryck ska få jämföras i Eurodacsystemet för brottsbekämpande ändamål är enligt artikel 20.1 i Eurodacförordningen att en jämförelse för att identifiera en registrerad först görs i nationella databaser, så långt det är möjligt i andra EU-medlemsstaters fingeravtryckssystem som används för tillämpning av Prümbesluten samt i informationssystemet för viseringar (VIS). Av de nationella databaserna kan dock inte polisens nationella register med fingeravtryck som registrerats med stöd av 131 § i utlänningslagen användas vid brottsbekämpning med stöd av den gällande lagen. Detta har setts som problematiskt med tanke på brottsbekämpningen. Problemet accentueras framför allt när det gäller att bekämpa terroristiska brott och andra brott som är samhälleligt betydelsefulla och har allvarliga följder och för vilka gäller att utredningsintressena är stora och att det är viktigt med förebyggande insatser.

Uppgifter för identifiering av utlänningar behandlas med stöd av utlänningslagen som en del av polisens övervakning av utlänningar. Jämförelse av fingeravtrycksuppgifter om utlänningar med fingeravtryck i signalementsuppgifterna i informationssystemet för polisärenden för att klarlägga förutsättningarna för inresa har möjliggjorts till den del registrerade signalementsuppgifter anknyter till ett brott för vilket det föreskrivna maximistraffet är fängelse i minst ett år. Den föreslagna utvidgningen till att gälla jämförelser i brottsbekämpningssyfte är betydande med tanke på integritetsskyddet för personer som registrerats med stöd av 131 § i utlänningslagen. Den föreslagna bestämmelsens förhållande till skydd för privatlivet och jämlikhetsprincipen enligt grundlagen bedöms närmare i kapitlen 4.1 och 4.2.

Det föreslagna 6 mom. begränsar på motsvarande sätt som den gällande 16 § användningen av uppgifter i en skjutvapenanmälan enligt 114 § i skjutvapenlagen till behandling av uppgifter som gäller vapentillstånd. Med detta avses på motsvarande sätt som i den gällande 10 § att uppgifterna i skjutvapenanmälningar får framgå av systemet bara när uppgifter som gäller vapentillstånd behandlas.

3 kap. Särskilda bestämmelser om behandling av personuppgifter

1 §. *Polisens rätt att få uppgifter ur vissa register och informationssystem.* I samband med 2013 års lagändringar (RP 66/2012 rd) ändrades polisens rätt att genom en teknisk anslutning få uppgifter ur vissa register för att motsvara den rätt att lämna ut uppgifter som den utlämnande instansen har. Bestämmelsen ändrades så att den omfattar också sådana uppgifter om resande som ansluter sig till hotell- och restaurangverksamhet, uppgifter ur gränsbevakningsväsendets och tullens personregister, uppgifter ur farkostregistret, uppgifter i anslutning till handräckningen av den myndighet som begärt handräckning och uppgifter ur försvarsmaktens värnpliktsregister. Bestämmelserna i 13 § preciserades i fråga om användningsändamål och informationsinnehåll. I motiveringen i regeringspropositionen fästes dock uppmärksamhet vid att lagen om behandling av personuppgifter i polisens verksamhet hade ändrats ett flertal gånger i samband med olika lagstiftningsprojekt. För en totalreform av den gällande lagen skulle det ha krävts en mera omfattande granskning och en utvärdering av lagstiftningstekniken i fråga om utlämnande och mottagande av uppgifter vid informationsutbyte mellan myndigheterna, och en sådan granskning och utvärdering hade inte varit möjlig att genomföra i det sammanhanget. Man beslutade därför ändra den gällande lagen, även om det delvis har lett till att rätten att lämna ut och få uppgifter har reglerats dubbelt.

Möjligheten att stryka bestämmelserna om rättigheterna att få information i polisväsendets personuppgiftslag har bedömts i samband med beredningen av lagförslag 1. De föreslås dock kvarstå tills vidare i enlighet med 2013 års lagändringar, bortsett från vissa preciseringar och föreslagna rättelser i de hänvisande bestämmelserna (1 mom.). I 16 punkten föreslås en hänvisning till den nya lagen om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (/), där det föreskrivs om rätt att få uppgifter ur flygtrafikens passagerarregister, till åtskillnad från 16 punkten som gäller alla transportörer i enskilda fall. Bland annat behovet att kvarhålla den rätt att få uppgifter avgiftsfritt som föreskrivs för polisen i 13 § i den gällande lagen talar för att rättigheterna att få information består. En sådan reglering saknas till stor del i bestämmelserna om utlämnande av uppgifter. En bestämmelse om avgiftsfrihet föreslås i 2 mom. Ett slopande av regleringen har till vissa delar bedömts som en lagtekniskt sett problematisk lösning också därför att en bestämmelse om utlämnande av uppgifter inte kan tas in i någon av de gällande speciallagarna. Också möjligheten enligt den gällande 13 § att förelägga vite i vissa situationer talar för att regleringen bör kvarstå. Bestämmelser om föreläggande av vite föreslås i 4 §.

I det föreslagna 3 mom. åläggs polisen skyldighet att ge den personuppgiftsansvarige som lämnat ut personuppgifter information om behandlingen av de personuppgifter som polisen fått. Polisen åläggs också skyldighet att säkerställa att de mottagna personuppgifterna behövs, om personuppgifter har lämnats ut utan begäran. Med ändrad ordalydelse motsvarar bestämmelsen 13 § 3 mom. i den gällande lagen.

2 §. *Uppgifter som andra myndigheter lämnar ut till polisen genom registrering vid direkt anslutning eller för registrering som en datamängd.* Till skillnad från kapitlets 1 §, som gäller utlämnande med en teknisk anslutning eller som en datamängd, föreskrivs det i 2 § om utlämnande av personuppgifter till polisen direkt eller som en datamängd. Förteckningen i 1 mom. motsvarar förteckningen i 14 § 1 mom. i den gällande lagen. I 2 mom. åläggs polisen på motsvarande sätt som i 1 § att ge den personuppgiftsansvarige som lämnat ut personuppgifter information om behandlingen av personuppgifterna samt säkerställa att de mottagna personuppgifterna behövs. Momentet motsvarar 14 § 2 mom. i den gällande lagen.

3 §. *Europeiska unionens informationssystem för viseringar.* I paragrafen föreskrivs det om polisens rätt att genom teknisk anslutning få uppgifter ur Europeiska unionens informationssystem för viseringar. Det föreslagna 1 mom. gäller mottagande av personuppgifter för utförande av en uppgift som enligt utlänningslagen ska skötas av polisen. I 2 mom. föreskrivs det om rätten att få uppgifter i syfte att förhindra och utreda terroristbrott och andra allvarliga brott. Bestämmelserna motsvarar 42 § i den gällande lagen.

4 §. *Vite.* Den föreslagna paragrafen ersätter 13 § 2 mom. i den gällande lagen. Genom det momentet har polisen getts befogenhet att ålägga samfund och sammanslutningar att inom en skälig tid ur register som gäller passagerare och fordons personal lämna uppgifter för förhindrande, avslöjande och utredning av brott och för överlämnande till åtalsprövning samt uppgifter som behövs för att efterlysta personer ska nås. Polisen föreslås på motsvarande sätt som enligt det gällande 13 § 2 mom. ha befogenhet att förena åläggandet med vite under de förutsättningar som anges i paragrafen.

4 kap. Utlämnande av personuppgifter ur polisens informationssystem

1 §. *Utlämnande av personuppgifter till en sådan behörig myndighet som avses i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.* I paragrafen beaktas de myndigheter som avses i dataskyddsdirektivet och som behandlar personuppgifter för ändamål som anges i 1 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, bortsett från försvarsmakten. I den föreslagna paragrafen avses sådana situationer för utlämnande av personuppgifter där den mottagande brottsbekämpande myndighetens behandling av personuppgifter alltid anses omfattas av dataskyddsdirektivets tillämpningsområde, till skillnad från 2 §, i fråga om vilken gäller att de myndigheter som avses i paragrafen behandlar personuppgifter till största delen inom dataskyddsförordningens tillämpningsområde. Bestämmelsen är ny, men i praktiken innebär den inte någon förändring av nuläget. Personuppgifter ska få lämnas ut till de myndigheter som avses i paragrafen också genom teknisk anslutning eller som en datamängd. I praktiken är utlämnande genom teknisk anslutning huvudregel i de situationer som avses i paragrafen.

I 1 mom. beaktas utlämnande av personuppgifter till andra brottsbekämpande myndigheter, nämligen Tullen och Gränsbevakningsväsendet. Momentet handlar om utlämnande av personuppgifter som anknyter till förebyggande, avslöjande och utredning av brott. Bestämmelser om utlämnande av personuppgifter till dessa myndigheter för andra ändamål med behandlingen föreslås i 2 §.

I det föreslagna 2 mom. preciseras sådana andra behöriga myndigheter inom dataskyddsdirektivets tillämpningsområde till vilka personuppgifter ska få lämnas ut för det ändamål som föreskrivs i 1 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Situationerna för utlämnande av uppgifter motsvarar i huvudsak 14 § 12, 14 och 15 punkten i den gällande lagen. I den föreslagna 1 punkten beaktas åklagarnas behandling av personuppgifter, i 2 punkten domstolarnas behandling av personuppgifter, i 3 punkten Rättsregistercentralens behandling av personuppgifter, i 4 punkten Brottspåföljdsmyndighetens behandling av personuppgifter och i 5 punkten justitieförvaltningsmyndigheternas och militärmyndigheternas behandling. Till skillnad från 1 mom. föreslås situationerna för behandling av personuppgifter bli preciserade för att grundlagsutskottets tolkningar om noggrant avgränsade bestämmelser om utlämnande av personuppgifter ska bli beaktade.

2 §. *Utlämnande av personuppgifter till andra myndigheter.* Innehållet i den föreslagna paragrafen motsvarar i huvudsak 14 § i den gällande lagen, bortsett från de situationer för utlämnande av personuppgifter som föreslås bli beaktade i 1 §. I paragrafen föreslås i analogi med de gällande bestämmelserna bestämmelser om andra myndigheter till vilka personuppgifter ska få lämnas ut ur polisens informationssystem. Till skillnad från de myndigheter som anges i den föreslagna 1 § handlar 2 § om myndigheter som utför sådan behandling av personuppgifter som i övrigt eller helt omfattas av tillämpningsområdet för den allmänna dataskyddsförordningen. I den föreslagna paragrafen föreskrivs det också om utlämnande av personuppgifter till behöriga myndigheter som avses i dataskyddsdirektivet till den del behandlingen omfattas av tillämpningsområdet för dataskyddsförordningen. EU:s dataskyddsdirektiv förutsätter att när personuppgifter behandlas för något annan än ett ändamål som omfattas av direktivets tillämpningsområde ska detta fastställas i lag. Enligt motiveringen till dataskyddsdirektivet omfattas dessa situationer alltid av dataskyddsförordningens tillämpningsområde.

I 1 mom. föreslås med beaktande av grundlagsutskottets ställningstaganden en uttömmande förteckning över de myndigheter till vilka personuppgifter ska få lämnas ut ur polisens informationssystem genom teknisk anslutning. I momentet anges också i detalj de ändamål med behandlingen av personuppgifter för vilka personuppgifter ska få lämnas ut.

I 2 mom. beaktas polisens behov av att i anslutning till ett visst uppdrag lämna ut personuppgifter även till andra myndigheter, exempelvis för att förebygga eller utreda ett brott. Informationsinnehållet i bestämmelsen är öppet, och för att uppgifterna ska få lämnas ut förutsätts det därför att de uppgifter som lämnas ut är nödvändiga för att en annan myndighet eller polisen ska kunna fullgöra sitt uppdrag. En sådan situation kan förekomma exempelvis när polisen lämnar ut personuppgifter om ett barns familjemedlem till en barnskyddsmyndighet. Det kan vara nödvändigt att lämna ut uppgifterna för att barnskyddsmyndigheten ska kunna bedöma om ett barn utsätts för våldshot i sitt hem innan barnskyddsmyndigheten fattar beslut om omhändertagande. På motsvarande sätt ska polisen kunna lämna ut personuppgifter exempelvis till Skatteförvaltningen för att skattebrott ska kunna förebyggas, avslöjas eller utredas. Utöver nödvändighetskriteriet för personuppgifter förutsätts det för utlämnande av de uppgifter som avses i momentet att utlämnandet inte medför uppenbar olägenhet för de intressen som sekretessen är avsedd att skydda. Paragrafen är en specialbestämmelse om utlämnande av personuppgifter trots tystnadsplikten i förhållande till 7 kap. 2 § i polislagen, där det föreskrivs om utlämnande av generellt sekretessbelagd information till myndigheter och sammanslutningar som sköter offentliga uppdrag.

I 3 mom. föreslås en begränsande bestämmelse enligt vilken fingeravtrycksuppgifter i pass trots sekretessbestämmelserna ska få lämnas ut endast till vissa i momentet preciserade myndigheter för styrkande av identitet och konstaterande av ett dokuments äkthet, när det behövs för behandling av ärenden som gäller en persons inresa, vistelse i landet eller utresa.

Mottagaren av personuppgifter ska enligt förslaget åläggas skyldighet att innan personuppgifter lämnas ut förelägga den personuppgiftsansvarige en tillförlitlig utredning om att uppgifterna skyddas på behörigt sätt (4 mom.). I 5 mom. föreskrivs det att kvaliteten på de uppgifter som lämnas ut ska bekräftas i den mån det är möjligt och att uppgifterna vid behov ska förses med information som gör det möjligt för mottagaren att bedöma hur korrekta, fullständiga, aktuella och tillförlitliga uppgifterna är. Utlämnande av felaktiga uppgifter och utlämnande i strid med lag ska också utan dröjsmål meddelas mottagaren. Avsikten är att kraven ska underlätta de personuppgiftsansvarigas arbete, med beaktande av deras ömsesidiga skyldigheter när det gäller att skydda personuppgifter och säkerställa att de är korrekta. De personuppgiftsansvariga ska också ta hänsyn till de särskilda förutsättningar som gäller för behandling av personuppgifter i dessa situationer och som grundar sig på lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och på den allmänna dataskyddsförordningen. Som exempel kan nämnas sådana begränsningar för användningen av personuppgifter mottagna från en annan myndighet eller en annan stat som det ska göras en anteckning om.

3 §. *Utlämnande av personuppgifter till privata sammanslutningar och personer.* I paragrafen beaktas polisens behov av att i vissa situationer lämna ut personuppgifter även till privata sammanslutningar och personer. Möjligheten att lämna ut personuppgifter begränsas enligt 1 mom. till situationer där utlämnandet är nödvändigt på grund av att saken är brådskande, att det är fråga om en farosituation, för att brott ska kunna förebyggas, egendom ska kunna återställas till ägaren eller av skäl som har samband med utredningen och utlämnandet av uppgifterna inte strider mot den registrerades legitima intresse. Sådana situationer kan anknyta till exempelvis kreditkortsbedrägerier eller bekämpning av it-brottslighet. Med bestämmelsen avses i fråga om verksamhet i datanät framför allt att det ska vara möjligt att be företag bekräfta datainnehåll som hänför sig till en IP-adress och att polisen då till företaget ska kunna lämna ut personuppgifter som är nödvändiga. Bestämmelsen motsvarar till sitt syfte artikel 29 i dataskyddsdirektivet. Den artikeln möjliggör utlämnande av personuppgifter till privata i noggrant avgränsade situationer. Artikeln i dataskyddsdirektivet gäller endast privata sammanslutningar i tredjeländer, men en motsvarande reglering är ändamålsenlig också för den nationella behandlingen av personuppgifter.

I 2 mom. föreskrivs det om polisens rätt att via allmänt datanät lämna ut personuppgifter för att allmänheten ska kunna underrättas och för att tips från allmänheten ska kunna fås. Innehållet i bestämmelsen motsvarar 19 a § i den gällande lagen. Via allmänt datanät ska på motsvarande sätt som för närvarande få lämnas ut endast uppgifter som måste tillkännages särskilt på grund av att saken är brådskande, att det är fråga om en farosituation, för att brott ska kunna förebyggas, egendom ska kunna återställas till ägaren eller av skäl som har samband med utredningen. Mängden personuppgifter som lämnas ut via allmänt datanät ska begränsas så att den är så liten som möjligt. Med stöd av bestämmelsen ska även biometriska uppgifter, framför allt ansiktsfotografier, få lämnas ut via datanätet.

I 3 mom. föreslås en hänvisande bestämmelse till 44 § i lagen behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Bestämmelserna i den paragrafen ska tillämpas när personuppgifter lämnas ut till privata sammanslutningar etablerade i tredjeländer.

4 §. *Utlämnande av personuppgifter till privata sammanslutningar eller näringsidkare via e-tjänster.* Bestämmelsen är ny. I paragrafen föreskrivs det om utlämnande av personuppgifter som anknyter till giltigheten av tillstånd till sådana privata sammanslutningar och näringsidkare för vilka det någon annanstans i lagstiftningen har föreskrivits uppgifter vilkas skötsel nödvändigtvis kräver behandling av uppgifter om giltigheten av tillstånd. Tillstånden inbegriper alla tillstånd och godkännanden, även resedokument, vilkas uppgifter polisen behandlar

för de ändamål som anges i 2 kap. 9 §. Rätten att lämna ut uppgifter föreslås i paragrafen begränsas till att gälla bara uppgifter om giltigheten av tillstånd. Med stöd av den föreslagna paragrafen ska inte andra tillståndsförvaltnings- och tillsynsuppgifter som behandlats med stöd av 9 § få lämnas ut via e-tjänster. Sättet att lämna ut uppgifter föreslås dessutom begränsas så att uppgifter får sökas endast som enskilda sökningar. Grundlagsutskottet har tolkat begränsningen som ett adekvat sätt att skydda utlämnandet av uppgifter via allmänt datanät. Paragrafen handlar inte om att uppgifter lämnas ut till allmänheten, utan till en avgränsad grupp av mottagare via e-tjänster som avgränsats genom kontrollen av användarrättigheterna. Begränsningen till enskilda sökningar utgör en garant för att uppgifterna skyddas och är följaktligen en skyddsåtgärd som säkerställer att integritetsskyddet tillgodoses. Behovet att kontrollera uppgifterna om giltigheten av tillstånd hänför sig också i praktiken alltid till situationer där den som har rätt att få information granskar giltigheten för en enskild persons tillstånd i kontaktsituationer på den registrerades initiativ, och därför finns det inga behov av att möjliggöra sökning av flera tillståndsuppgifter på en gång.

Privata sammanslutningar och näringsidkare som är mottagare föreslås inte bli specificerade i paragrafen, utan mottagarna avgränsas utifrån de uppgifter som föreskrivs någon annanstans i lagstiftningen. Med stöd av paragrafen ska uppgifter få lämnas ut till exempelvis innehavare av ett näringstillstånd i vapenbranschen för fullgörande av anmälningsskyldigheten i 42 c § i skjutvapenlagen och i samband med vilket innehavaren av näringstillståndet kompletterar tillståndsuppgifterna med identifieringsuppgifter om skjutvapen eller vapendelar via e-tjänster (RP 266/2016 rd). De situationer som avses i paragrafen omfattar också sådant utlämnande av information om giltighet för pass eller identitetskort till leverantörer av identifieringstjänster som anges i 7 b § i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Den föreslagna paragrafen möjliggör utlämnande av uppgifter också i sådana situationer som senare tas in i speciallagstiftning där det för privata sammanslutningar eller personer föreskrivs uppgifter för vilkas skötsel det är nödvändigt att kontrollera uppgifter om giltigheten för tillstånd. Den personuppgiftsansvarige ska dock alltid ha rätt att besluta om utlämnande, och paragrafen medför således inte någon skyldighet för polisen att lämna ut personuppgifter.

Behandling av personuppgifter inom det internationella samarbetet

Genom 2013 års lagändringar (RP 66/2012 rd) fick bestämmelserna om behandling av personuppgifter inom det internationella polissamarbetet en annan utformning. Till lagen fogades nya bestämmelser om behandlingen av information från utlandet. Lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet preciserades med motsvarande ändringar som polisväsendets personuppgiftslag. Genom lagändringarna genomfördes också till kompletterande delar de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete inom inrikesministeriets förvaltningsområde. Det föreslås att innehållet i dessa bestämmelser ska kvarstå i huvudsak utan ändringar. I 4 kap. i lagförslag 1 beaktas utöver utlämnanden av information mellan de brottsbekämpande myndigheterna i medlemsstaterna också i likhet med den gällande lagen de EU-omfattande informationssystem som dessa myndigheter använder.

5 §. *Utlämnande av personuppgifter till tillsynsmyndigheter i Europeiska unionens medlemsstater.* I 1 mom. beaktas den så kallade principen om tillgång till information, enligt vilken de brottsbekämpande myndigheterna i andra EU-medlemsstater ska ha rätt att få personuppgifter och andra uppgifter under samma förutsättningar som de står till förfogande för polisen för förebyggande, avslöjande och utredning av brott. Innehållet i bestämmelsen motsvarar 29 § i den gällande lagen. Också personuppgifter som lagrats i register som anknyter till tillståndsä-

renden ska få lämnas ut under samma förutsättningar som enligt den gällande lagen. Uppgifterna ska få lämnas elektroniskt eller som en datamängd. Polismyndigheterna i EU-medlemsstaterna använder en skyddad kanal för utbyte av information.

I 2 mom. föreslås en informativ hänvisning till lag 26/2009 som gäller tillämpning av rambeslutet 2006/960/RIF och föreskriver om utbyte av information och underrättelser mellan brottsbekämpande myndigheter i syfte att säkerställa att rambeslutet har genomförts på behörigt sätt när det gäller utlämnande av personuppgifter. Lagen om genomförande av rambeslutet är en specialförfattning i förhållande till lagförslaget.

6 §. *Utlämnande av personuppgifter ur det nationella systemet inom Schengens informationssystem.* I Schengens informationssystem ingår ett nationellt system, och i den föreslagna paragrafen beaktas utlämnandet av personuppgifter ur det nationella systemet. Bestämmelsen är informativ och motsvarar 35 § i den gällande lagen.

7 §. *Utlämnande av personuppgifter till Schengenstater och Schengens informationssystem.* I paragrafen föreskrivs det om polisens rätt att lämna ut uppgifter om efterlysningar till Schengenstaternas behöriga myndigheter och för registrering i Schengens informationssystem. Bild- och fingeravtrycksuppgifter i anslutning till efterlysningar ska överföras via det nationella systemet inom Schengens informationssystem. Tilläggsinformation ska lämnas ut genom förmedling av Sirenekontoret. Paragrafen motsvarar 36 § i den gällande lagen.

8 §. *Utlämnande av uppgifter till Europols informationssystem.* Europaparlamentets och rådets förordning (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (Europolförordningen) och den lag (214/2017) som kompletterar den trädde i kraft den 1 maj 2017. I paragrafen föreslås informativa bestämmelser som kompletterar förordningen och lagen och som gäller utlämnande av personuppgifter till de informationssystem som används till i kapitel IV i Europolförordningen avsedd behandling av uppgifter. Enligt 1 mom. ska det få sättas begränsningar för användningen av de personuppgifter som lämnas ut eller för vidare överlåtelse av personuppgifterna.

I 2 mom. preciseras de kanaler som ska användas för utlämnande av personuppgifter och i 3 mom. föreskrivs det om rätt för centralen för utredning av penningtvätt vid centralkriminalpolisen att inom ramen för sina uppdrag lämna ut personuppgifter till Europol via den nationella enheten. Den explicita bestämmelsen beaktar att det i Europols uppgifter ingår framför allt att stödja medlemsstaternas brottsbekämpande organ med att förebygga och bekämpa gränsöverskridande brott. Till sådana brott hänförs även penningtvätt och terroristbrott, där även finansiering av terrorism ingår. Europolförordningen ålägger medlemsstaternas finansunderrättelseenheter (centraler för utredning av penningtvätt) att samarbeta med Europol. Rätten att lämna ut personuppgifter i anknytning till detta säkerställs genom den föreslagna bestämmelsen.

9 §. *Utlämnande av personuppgifter till Eurodacsystemet.* Bestämmelsen motsvarar den informativa bestämmelsen 39 § i den gällande lagen, men hänvisningarna föreslås bli ändrade för att motsvara ändringarna i EU-lagstiftningen. I den föreslagna paragrafen föreskrivs det om polisens rätt att lämna ut fingeravtrycksuppgifter och andra personuppgifter till Eurodacsystemet för jämförelse av fingeravtrycksuppgifter. Det ändamål med användningen av uppgifterna i Eurodacsystemet som avsågs i rådets förordning (EG) nr 2725/2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen utvidgades genom Europaparlamentets och rådets förordning (EU) nr 603/2013 (Eurodacförordningen), som började tillämpas den 20 juli 2015. Förordningen innebär att fingeravtryck som registrerats i Eurodacsystemet kan användas för brottsbekämpande ändamål

när det gäller att bekämpa terroristbrott och andra allvarliga brott. I paragrafen föreslås dessutom en bestämmelse om att centralkriminalpolisen är den utsedda myndighet för brottsbekämpande ändamål som avses i artikel 5.1 i Eurodacförordningen.

10 §. *Utlämnande av personuppgifter med stöd av Prümfördraget och Prümrådsbeslutet.* Genom paragrafen sätts bestämmelserna i Prümfördraget och Prümrådsbeslutet i kraft till den del det är fråga om att med stöd av fördraget och beslutet lämna ut personuppgifter till följd av brott. Paragrafen motsvarar i huvudsak 40 § i den gällande lagen. Den informativa bestämmelsen om utplåning av personuppgifter som finns i den gällande paragrafen föreslås bli flyttad till 5 kap. och bestämmelsen om den registrerades rätt till insyn föreslås bli beaktad i 8 kap.

I det föreslagna 1 mom. föreskrivs det om så kallad sökning som lett till en träff av DNA-uppgifter, fingeravtrycksuppgifter och fordonsregisteruppgifter. För dessa använder EU-medlemsstaterna sig av ett decentraliserat system där polisen kan göra sökningar som leder till träffar bland referensuppgifter i det aktuella registret i en annan medlemsstat.

I 2 mom. föreslås en informativ bestämmelse som preciserar de tillämpliga bestämmelserna på utbyte av information efter den uppgift om träff som avses i 1 mom. Bestämmelsen är ny och det är meningen att den ska skapa klarhet i förhållandet mellan Prümrådsbeslutet och den övriga lagstiftningen. Rådets beslut 2008/615/RIF överlåter besluten om förfarandet och kanalen för utbyte av information till medlemsstaternas brottsbekämpande myndigheter, och därför är det ändamålsenligt att förfarandet och kanalen preciseras genom hänvisningar på lagnivå. Målet med detta är att säkerställa att Prümfördraget och Prümrådsbeslutet sätts i kraft på ett effektivt sätt samt att rådets rambeslut 2006/960/RIF genomförs på ett effektivt sätt.

11 §. *Utlämnande av personuppgifter till tredjeland eller till den internationella kriminalpolisorganisationen.* Paragrafen motsvarar i huvudsak 30 § i den gällande lagen. Enligt förslaget stryks dock sådana bestämmelser som kommer att finnas i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Dessutom föreslås det att bestämmelserna om utlämnande av personuppgifter i överensstämmelse med det ursprungliga ändamålet med behandlingen tas in i kapitlets 12 §. På utlämnande av personuppgifter till tredjeländer och till internationella organisationer ska till alla delar tillämpas 7 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, bortsett från skyddspolisens informationsutbyte, om vilket det föreskrivs särskilt i 7 kap. i lagförslag 1. Lagen om centralen för utredning av penningtvätt samt till kompletterande delar 7 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska tillämpas på utbyte av personuppgifter mellan centralen för utredning av penningtvätt och tredjeländer. Den föreslagna paragrafen innehåller närmare bestämmelser om dessa för att precisera vilka personuppgifter som får lämnas ut till tredjeländer och till internationella organisationer och för att precisera att med internationell organisation inom polissamarbetet avses den internationella kriminalpolisorganisationen (I.C.P.O. - Interpol). Preciseringen behövs eftersom Interpol inte är en internationell organisation i den bemärkelse som internationell organisation definieras i EU:s dataskyddsförordning och dataskyddsdirektiv, men i ingressen till direktivet preciseras att direktivets bestämmelser om överföring av personuppgifter till tredjeländer och till internationella organisationer kan tillämpas också inom samarbetet med Interpol. I praktiken har polisen inga behov av att lämna ut personuppgifter direkt till andra internationella organisationer än till Interpol. I 1 mom. preciseras för vilka ändamål med behandlingen registrerade personuppgifter ska få lämnas ut till Interpol och till brottsbekämpande myndigheter i de stater som är medlemmar i Interpol. Interpol och dess medlemsstater har en skyddad kanal för elektronisk utlämning av uppgifter.

I 2 mom. preciseras för vilka ändamål med behandlingen registrerade personuppgifter ska få lämnas ut till andra tredjeländer. Under de förutsättningar som preciseras i lagen ska person-

uppgifter som omfattas av samma ändamål med behandlingen i princip få lämnas ut till alla tredjeländer. Enligt 3 mom. ska det få sättas begränsningar och ställas villkor för användningen av de personuppgifter som lämnas ut. Polisen ska också kunna vägra lämna ut uppgifter, om det kan vara till skada för arbetet med att förebygga, avslöja eller utreda brott eller föra brott till åtalsprövning, eller av någon annan grundad anledning. Sådana anledningar kan utgöras av ovillkorliga grunder för vägran, framför allt potentiell tortyr och potentiellt dödsstraff. För alla tredjeländer bör det beaktas att den nivå på dataskyddet som avses i dataskyddslagstiftningen inte automatiskt är tillräckligt hög, utan den kan anses vara tillräckligt hög i de situationer som preciseras i 7 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Dataskyddsnivån kan också förändras. Personuppgifter ska få lämnas ut till tredjeländer och till Interpol endast om dessa säkerställer en tillräcklig nivå på dataskyddet i enlighet med vad som föreskrivs i den nämnda lagen. I 7 kap. i den lagen ingår dock bestämmelser om undantag utifrån vilka personuppgifter får lämnas ut i enskilda fall, om det är nödvändigt för att förebygga, förhindra, avslöja och utreda brott. Vid utlämnande av uppgifter gäller det också att beakta övriga krav i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Ett sådant krav är att personuppgifter som har erhållits från en EU-medlemsstat endast i avgränsade situationer får vidareöverföras till ett tredjeland eller Interpol utan samtycke på förhand. Sådana situationer anknyter till avvärjande av ett omedelbart och allvarligt hot mot den allmänna säkerheten eller mot Finlands väsentliga intressen. I dessa situationer ska den medlemsstat som lämnat ut personuppgifterna informeras om vidare överlåtelsen utan dröjsmål.

I 4 mom. föreskrivs det om rätt att lämna ut personuppgifterna elektroniskt eller som en datamängd. I momentet föreslås också en informativ hänvisning till internationell rättslig hjälp i brottmål.

12 §. *Utlämnande av personuppgifter till tredjeland eller till den internationella kriminalpolisorganisationen i överensstämmelse med det ursprungliga ändamålet med behandlingen.* I paragrafen föreskrivs det om vissa specialsituationer som anses vara sådana ändamål med behandlingen av personuppgifter som står i överensstämmelse med sådan behandling av personuppgifter som omfattas av tillämpningsområdet för lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I enlighet med 1 mom. ska utlämnande av personuppgifter till de behöriga myndigheter som avses i internationella avtal eller andra arrangemang som gäller återtagande av personer som olagligen kommit in och vistas i landet för utförande av de uppdrag som avses i de internationella avtalen eller arrangemangen anses stå i överensstämmelse med den ursprungliga behandlingen.

I 2 mom. föreslås en begränsande bestämmelse som gäller utlämnande av fingeravtrycksuppgifter i pass. Fingeravtrycksuppgifter i pass ska få lämnas ut till ett tredjeland eller till den internationella kriminalpolisorganisationen endast på det sätt som föreskrivs i 2 kap. 11 § 4 mom. Bestämmelsen motsvarar 30 § 3 mom. i den gällande lagen. I det föreslagna 3 mom. föreskrivs det om utlämnande till de myndigheter som ansvarar för vapentillsynen i en annan stat av sådana personuppgifter som är nödvändiga med tanke på vapentillsynen. Bestämmelsen motsvarar 30 § 4 mom. i den gällande lagen.

13 §. *Behandling av personuppgifter som fåtts från ett tredjeland, den internationella kriminalpolisorganisationen eller någon annan internationell brottsbekämpande myndighet.* Bestämmelsen motsvarar delvis 31 § i den gällande lagen. Det föreslås dock att de gällande bestämmelserna i 31 § 3–5 mom. stryks som obehövliga, eftersom de krav som anges i dem kommer att ingå i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I det föreslagna 1 mom. föreskrivs det i analogi med 31 § 1 mom. i den gällande lagen om sekretess och tystnadsplikt samt om skyldigheten att iaktta de

begränsningar för användningen av personuppgifter som den som lämnar ut uppgifterna har ställt. Momentet innehåller en huvudregel som syftar till att säkerställa förtroendeskyddet.

I 2 mom. föreskrivs det om möjligheten att använda mottagna personuppgifter för andra ändamål än det ursprungliga ändamålet, om det inte har ställts några begränsningar enligt 1 mom. och något av de villkor som nämns i 2 mom. är uppfyllda. Innehållet motsvarar 31 § 2 mom. i den gällande lagen, men det föreslås att 1 punkten ändras så att formuleringen bättre motsvarar bestämmelsen om dataskyddsdirektivets tillämpningsområde.

14 §. *Beslut om utlämnande av uppgifter.* I paragrafen föreskrivs det om beslutsfattande som gäller rätten att som en datamängd eller genom teknisk anslutning lämna ut uppgifter ur polisens personregister till myndigheter som avses i 1 och 2 § samt om rätten för de myndigheter som avses i 3 kap. att på dessa två sätt lämna ut uppgifter till polisens informationssystem (1 mom.). Besluten ska fattas av den personuppgiftsansvarige eller av en annan polisenhet som den personuppgiftsansvarige har förordnat till uppdraget. Enligt 2 mom. ska uppgifternas art beaktas när beslut om utlämnande fattas.

Att öppna en teknisk anslutning innebär ett mer långtgående utlämnande av uppgifter än när personuppgifter lämnas ut separat på begäran av en annan myndighet. När uppgifter lämnas ut genom en teknisk anslutning är det också svårare för den personuppgiftsansvarige att övervaka hur personuppgifterna skyddas och används, och därför ska det i enlighet med 2 § 4 mom. krävas att den andra myndigheten lägger fram en utredning om att personuppgifterna skyddas på behörigt sätt innan den tekniska anslutningen öppnas. Med hänsyn till de skyldigheter som den nya dataskyddslagstiftningen medför för de personuppgiftsansvariga är det också ändamålsenligt att dessa får verktyg för att övervaka. Den personuppgiftsansvarige ska i varje enskilt fall kunna bedöma om det är motiverat att öppna en teknisk anslutning och om den annars kan öppnas.

5 kap. Utplåning, kontroll och arkivering av personuppgifter

Genom lagändringen 2013 (RP 66/2012 rd) ändrades bestämmelserna om utplåning av personuppgifter för att motsvara den förändrade omvärlden. Uppgifterna i polisens informationssystem ska enligt motiveringen bevaras enligt vad användningsbehovet kräver, med beaktande av kraven på rättssäkerhet för registrerade, andra parter eller personer som hör till polispersonalen. Förvaringstiden för uppgifter föreslogs vara fem år i fråga om lindrigare brott, besöksförbud och näringsförbud samt för tagande i förvar enligt polislagen av bland annat rusmedelspåverkade, medan det i fråga om grövre brott föreslogs bero på straffskalan för brottet. För de lagändringar som trädde i kraft 2013 gällde en övergångstid på fyra år, vilket grundade sig på att det inte var ändamålsenligt att genomföra ändringarna av bestämmelserna om utplåning i det gamla systemet på grund av höga kostnader, eftersom informationssystemet för polisärenden var under ombearbetning. Beträffande 22 § föreslås en förlängning av övergångstiden med två år (RP 181/2017 rd).

1 §. *Utplåning av personuppgifter som anknyter till brottmål.* Med beaktande av målet för lagändringarna 2013 föreslås det inte några ändringar i tiderna för utplåning av personuppgifter som anknyter till brottmål. Förvaringstiderna för personuppgifter ska fortfarande differentieras med avseende på hur grov gärning det är fråga om. Dessutom ska det tas hänsyn till att minderåriga som gjort sig skyldiga till brottsliga gärningar är i en mer utsatt ställning. Paragrafen omfattar utplåningen av personuppgifter som samlats in för förundersökningsändamål.

I enlighet med 1 mom. i paragrafen ska uppgifterna i ett brottmål utplånas när fem år har förflutit sedan brottmålet överfördes till åklagare, om det grövsta misstänkta brottet kan leda till böter, när tio år har förflutit, om det grövsta misstänkta brottet i brottmålet kan leda till ett

fängelsestraff på högst fem år, och när tjugo år har förflutit, om det grövsta misstänkta brottet i brottmålet kan leda till fängelse i över fem år. Enligt 2 mom. ska uppgifterna i övriga brottmål utplånas när ett år har förflutit sedan åtalsrätten för det senaste misstänkta brottet preskriberats, dock tidigast när fem år har förflutit sedan brottmålet registrerades. Enligt 3 mom. utplånas uppgifterna dock inte, om åtalsrätten inte har preskriberats.

I 4 mom. föreskrivs om utplåning av signalement och andra personuppgifter som registrerats för identifiering av personer som misstänks för brott, för utredning av brott och för registrering av gärningsmän. Dessa ska utplånas senast när tio år har förflutit sedan den sista uppgiften om den som är misstänkt för brottet infördes. Uppgifterna ska dock utplånas senast tio år efter den registrerades död, om det strängaste föreskrivna straffet för det grövsta brott som använts som grund för registrering är fängelse i minst ett år. Uppgifterna utplånas senast när fem år har förflutit sedan anteckningen infördes, om det i samband med undersökning framgår att inget brott har begåtts.

Paragrafens 5 mom. innehåller en hänvisning till Prümfördraget och Prümrådsbeslutet. För tillämpningen av Prümfördraget och Prümrådsbeslutet har EU:s medlemsstater infört informationssystem för sökning enligt principen om träff/icke träff för utbyte av information ur fordonsregister, fingeravtrycksuppgifter och DNA-profiler. I bestämmelserna i momentet föreskrivs om bevarandet av logguppgifter och övervakningsuppgifter och om tiderna för utplåning av uppgifterna i fråga.

I 6 mom. i paragrafen föreskrivs om undantag från tiderna för utplåning. Uppgifterna får bevaras, om de behövs för att behandla ett ärende, utföra ett uppdrag eller för att trygga rättigheterna för den registrerade, någon annan part eller en person som hör till polispersonalen. Uppgifterna kan således bevaras till exempel under en pågående undersökning av tjänstebrott. I momentet föreskrivs också om skyldigheten att regelbundet bedöma behovet av att bevara uppgifterna.

I 7 mom. beaktas minderåriga som begått brott. Uppgifter om registrerade som var under 15 år gamla då de begick brottet utplånas när den registrerade fyller 18 år, om inte den registrerade har gjort sig skyldig till en brottslig gärning efter att ha fyllt 15 år. Uppgifterna kan dock undantagsvis bevaras, om brottmålet gäller andra misstänkta för den brottsliga gärningen och uppgifterna om dem ännu inte ska utplånas eller om någon av anteckningarna gäller en brottslig gärning för vilken det inte föreskrivs någon annan påföljd än fängelse. Syftet med momentet är att säkerställa att barnens intressen beaktas i enlighet med konventionen om barnets rättigheter.

2 §. *Utplåning av personuppgifter som behandlas för andra i 2 kap. 3 och 5 § avsedda ändamål.* Bestämmelsen omfattar tiderna för utplåning av personuppgifter som behandlats för andra utredningsändamål än förundersökning. Med beaktande av uppgifternas nära anknytning till upprätthållande av allmän ordning och säkerhet bör också de personuppgifter som behandlats för ändamålet tas upp i samma paragraf. Det skulle vara tekniskt svårt att hålla isär uppgifterna i informationssystemet. Det föreslås att bestämmelserna om utplåning förenklas jämfört med 22 § i gällande lag som handlar om utplåning av uppgifter ur informationssystemet för polisärenden. Enligt 1 mom. i paragrafen får personuppgifter som behandlats för andra ändamål än förundersökning bevaras i fem år efter att anmälan eller ärendet registrerades. Avvikande från detta ska säkerhetsinformation utplånas senast ett år efter den registrerades död. På detta sätt gör man det möjligt att bevara uppgifterna om en person som bedöms som farlig så länge som det är nödvändigt för att trygga säkerheten för personen själv eller polisens personal. Med avvikelse från gällande bestämmelser föreslås det ingen särskild bestämmelse om utplåning av uppgifter som gäller efterspanade fordon och egendom. Uppgifterna utplånas när

de inte längre behövs för att behandla ett ärende, utföra ett uppdrag eller för att trygga rättigheterna för den registrerade, någon annan part eller en person som hör till polispersonalen.

I 2 mom. i paragrafen föreskrivs om avvikande tider för bevarande av uppgifter som anknyter till annan lagstiftning. Dessa gäller näringsförbud, besöksförbud, övervakad frihet på prov och övervakningsstraff. I 3 mom. föreskrivs om tiderna för utplåning av uppgifter om informationskällor, och i 4 mom. om tiderna för utplåning av uppgifter för identifiering av utlänningar. Huvudregeln för utplåning av uppgifter för identifiering av utlänningar är tio år efter att anteckningen infördes, förutom om den registrerade har beviljats finskt medborgarskap, då identifieringsuppgifterna ska utplånas när ett år har förflutit sedan den personuppgiftsansvarige fått kännedom om medborgarskapet. Alla uppgifter för identifiering av en utlänning ska dock utplånas senast ett år efter den registrerades död, om det inte finns särskilda skäl att fortfarande bevara dem för att behandla ett ärende, utföra ett uppdrag eller trygga rättigheterna för den registrerade, någon annan part eller en person som hör till polispersonalen. Behovet av att bevara personuppgifterna ska bedömas minst vart femte år.

3 §. *Utplåning av personuppgifter som anknyter till kriminalunderrättelseinhämtning och av observationsuppgifter.* Med beaktande av kriminalunderrättelseinhämtningens och observationsuppgifternas karaktär och deras inverkan på de grundläggande fri- och rättigheterna tas bestämmelserna om tiderna för utplåning av dem upp i en särskild paragraf.

Enligt 1 mom. ska personuppgifter som anknyter till kriminalunderrättelseinhämtning utplånas senast när tio år har förflutit sedan den sista uppgiften infördes i informationssystemet. När dessa uppgifter bevaras bör det särskilt uppmärksammas att den registrerades integritetsskydd och personliga frihet utsätts för en långtgående begränsning vars nödvändighet bör bedömas vart tredje år. Trots det berörs paragrafen också av de allmänna bestämmelserna om nödvändigheten av att behandla personuppgifter i 6 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

För observationsuppgifter är enligt 2 mom. förvaringstiden kortare. Observationsuppgifter ska utplånas senast när sex månader har förflutit sedan anteckningen infördes i informationssystemet. På detta sätt fästs uppmärksamheten vid att observationsuppgifter är osäkra till sin natur och inte ska förvaras längre än vad som är nödvändigt.

Enligt 3 mom. gäller en kortare förvaringstid också för de uppgifter i 2 kap. 7 § 2 mom. som inte hänför sig till ett visst uppdrag och som behandlas för att klarlägga om uppgifterna är nödvändiga. Uppgifter som konstaterats vara onödiga ska utplånas utan dröjsmål, dock senast när sex månader har förflutit sedan anteckningen infördes i informationssystemet. Bild- och ljudupptagningar som gjorts med hjälp av tekniska hjälpmedel ska dock utplånas senast när 96 timmar har förflutit sedan anteckningen infördes i informationssystemet. Uppgifter som bedöms vara nödvändiga och som uppfyller de villkor för behandling som anges i 3–6 § ska hänföras till denna behandlingskategori och följer då också de tider för förvaring som föreskrivs för uppgifterna i 3–6 §.

4 §. *Utplåning av personuppgifter som behandlas för utförande av tillståndsförvaltnings- och tillsynsuppgifter och uppgifter enligt hittegodslagen.* Bestämmelsen ersätter 23 § i den gällande lagen med undantag för uppgifter som används för identifiering av utlänningar. Bestämmelser om utplåningen av dessa ingår i 2 §. Gällande bestämmelser om utplåning av uppgifter har införts i samband med lagändringarna 2013. Bestämmelserna har dock till viss del visat sig vara problematiska med tanke på polisens uppgifter inom tillståndsförvaltningen. I bestämmelserna anges olika tidsfrister för utplåning av olika kategorier av uppgifter som gäller samma tillståndsärende, vilket har setts som ett problem med tanke på uppgifternas integritet. Dessutom har bestämmelserna ansetts vara oklara och komplicerade. En situation som in-

nebär problem för uppgifternas integritet är till exempel kravet på olika tider för utplåning av uppgifterna om beslut och tillstånd. Det föreslås att bestämmelserna om utplåning ändras så att personuppgifter som behandlats för utförande av tillståndsförvaltningsuppgifter som regel ska utplånas senast när tjugo år har förflutit sedan beslutet fattades eller förföll, den i beslutet angivna giltighetstiden gick ut eller personuppgiften infördes (1 mom.). En förenkling av bestämmelsen stärker den registrerades rättssäkerhet och bidrar i sin tur till att göra regleringen av behandlingen av personuppgifter tydligare och mindre tungrodd och komplicerad på det sätt som förutsätts av grundlagsutskottet (till exempel GrUU 31/2017 rd, GrUU 46/2016 rd, GrUU 71/2014 rd). Tiden för förvaring av uppgifter om identitetskort och pass, bilduppgifter, uppgifter som gäller tillsynen över säkerhetsbranschen samt tillsynen över penninginsamlingar och lotterier förlängs enligt det föreslagna 1 mom. till tjugo år. Den nuvarande förvaringstiden på tio år för uppgifter om identitetskort och pass har visat sig vara för kort när uppgifterna behövs för prövning av en persons förutsättningar att få behålla sitt medborgarskap. Tack vare den senaste tidens informationstekniska utveckling finns det inte längre något behov av att av tekniska skäl begränsa förvaringstiden för bilduppgifter så att den blir kortare än den för tillståndsärenden. En förlängning av förvaringstiden för uppgifter som gäller tillsynen över säkerhetsbranschen samt tillsynen över penninginsamlingar och lotterier förbättrar möjligheterna till uppföljning av tillståndens hela livscykel och insamling av nödvändiga uppgifter om övervakningshändelser. När det gäller tillstånden för penninginsamlingar och lotterier talar också lagstiftningen om villkoren för beviljandet av tillstånden i fråga för en förlängning av förvaringstiden. I lagstiftningen förutsätts det att uppgifterna för tidigare tillstånd beaktas vid tillståndsprövningen.

I 2 mom. i paragrafen föreskrivs det om undantag från den förvaringstid på tjugo år som anges i 1 mom. I 1 punkten i momentet föreskrivs, liksom i gällande lag, om en förvaringstid på tre år för uppgifterna i en skjutvapenanmälan enligt skjutvapenlagen. I 2 punkten beaktas den skyldighet som åläggs medlemsstaterna i Europaparlamentets och rådets direktiv (EU) 2017/853 av den 17 maj 2017 om ändring av rådets direktiv 91/477/EEG om kontroll av förvärv och innehav av vapen om en förvaringstid för uppgifterna på trettio år. I 3 punkten anges en kortare förvaringstid på ett år för personuppgifter som anknyter till hittegodsverksamhet. Under loppet av den tiden ska uppgifterna utplånas. Behandlingen av personuppgifter om ägaren eller upphittaren av hittegods är till sin natur kortvarig, och i samband detta fattas det inte några förvaltningsbeslut som kräver längre förvaringstid.

I 2 mom. 4 punkten föreskrivs det om utplåning av personuppgifter med anknytning till tillsynsuppdrag enligt 7 kap. i lagen om förhindrande av penningtvätt och av finansiering av terrorism. Bestämmelser om utplåning av personuppgifter som ingår i sådana rapporter om misstanke om överträdelser som avses i 7 kap. 9 § finns i 2 mom. i paragrafen (fem år efter att anteckningen infördes). För tydlighetens skull föreslås det att också övriga personuppgifter som anknyter till tillsynen enligt kapitlet i fråga utplånas senast när fem år har förflutit sedan anteckningen infördes. I 5 punkten i momentet föreskrivs dock om en kortare förvaringstid för personuppgifter som ska behandlas med anledning av tillsynen enligt lotterilagen eller lagen om förhindrande av penningtvätt och av finansiering av terrorism och som gäller kunder hos penningspelsbolag eller deras ombud . Dessa uppgifter ska utplånas genast när de inte längre behövs för utförande av tillsynsuppdraget. På detta sätt försäkrar man sig om att tillsynen inte inriktar sig på kunderna utan på penningspelsbolaget.

I 3 mom. i paragrafen föreskrivs på samma sätt som i nuvarande 23 § 2 mom. om utplåningen av personuppgifter senast ett år efter den registrerades död förutom i vissa undantagsfall. Bestämmelsen ska dock inte gälla de uppgifter som avses i 2 mom. 2–5 punkten. Den förvaringstid på trettio år som förutsätts i vapendirektivet kommer enligt direktivet inte att begränsas med anledning av personens död, eftersom behovet av långvarig förvaring av personuppgifterna för vapnets innehavare och ägare grundar sig på uppföljningen av vapnets livscykel.

Uppgifter som anknyter till hittegodsverksamhet ska enligt bestämmelsen i fråga utplånas senast när ett år har förflutit efter att anteckningen infördes, varvid bestämmelserna i 3 mom. saknar betydelse när det gäller förvaringstiden för uppgifterna. Paragrafen i fråga, som inte föreskriver om utplåning av uppgifter med anledning av den registrerades död, ska tillämpas på sådana rapporter om misstanke om överträdelser som avses i 7 kap. 9 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism. Å andra sidan ska det inte vara möjligt att med anledning av kundens död samla uppgifter ur det informationsmaterial som penningspelsbolaget lämnat till polisen för behandling av uppgifter om kunderna med tanke på den tillsyn som avses lagen om förhindrande av penningtvätt och av finansiering av terrorism. Uppgifterna ska inte kunna kopplas till en enskild fysisk person enbart utifrån de uppgifter som penningsspelsbolaget överfört till polisen i form av en datamängd, utan polisen ska få information om enskilda spelares identitet bara via penningspelsbolaget.

6 §. *Uppgifter som konstaterats vara felaktiga.* Paragrafen överensstämmer med innehållet i 27 § i gällande lag. Bestämmelsen gör det möjligt att bevara en felaktig uppgift tillsammans med den korrigerade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en person som hör till polispersonalen (1 mom.). Felaktiga uppgifter får användas bara för det syfte som här avses. Paragrafen ersätter inte kravet på begränsning av behandlingen av personuppgifter enligt 25 § 2 mom. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, utan genom att behålla paragrafen i oförändrad form säkerställer man en problemfri övergång till reglering enligt den nya lagen.

Dessutom kompletterar bestämmelsen det som föreskrivs i 2 kap. 9 § om behandlingssyfte beträffande den registrerades rätt enligt dataskyddsförordningen att få felaktiga personuppgifter rättade (artikel 16) och rätt till begränsning av behandlingen av personuppgifter (artikel 18). Enligt artikel 16 i förordningen ska den registrerade ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få inexakta och felaktiga personuppgifter som rör honom eller henne rättade. Paragrafen begränsar inte rätten att få uppgifter rättade, men uppgifter som konstaterats vara felaktiga kan i situationer som avses i 1 mom. bevaras tillsammans med de rättade uppgifterna. Enligt artikel 18.1 c ska den registrerade ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Enligt paragrafen tillåts det att en felaktig uppgift bevaras såväl i de fall som avses i artikel 18 som andra fall, om det är nödvändigt för att trygga rättigheterna för den registrerade, någon annan part eller en person som hör till polispersonalen.

I 2 mom. i paragrafen föreskrivs om undantag från rätten att bevara en felaktig uppgift, vilket gäller det nationella systemet inom Schengens informationssystem. Enligt 3 mom. ska en uppgift som konstaterats vara felaktig utplånas genast när den inte längre behövs för att trygga rättigheterna, dock senast när fem år har förflutit sedan den föreskrivna tiden för utplåning av uppgiften gått ut.

7 §. *Arkivering av uppgifter*. Paragrafen innehåller en informativ bestämmelse som hänvisar till arkivlagen (831/1994). Bestämmelsen överensstämmer med 28 § i gällande lag.

6 kap. **Den registrerades rättigheter**

Bestämmelserna om den registrerades rättigheter ingår huvudsakligen i 4 kap. i lagen om behandling av personuppgifter i brottmål och i III kap. i den allmänna dataskyddsförordningen. I detta kapitel preciseras bestämmelserna om den registrerades rätt till insyn och inskränkningar i rätten till insyn.

De skyldigheter som den registrerade har och som ska tillämpas vid behandlingen av personuppgifter fastställs i dataskyddsförordningen till viss del enligt den föreskrivna rättsliga grunden. Rätten till radering av uppgifter enligt artikel 17 tillämpas inte om syftet är att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige. Rätten till dataportabilitet enligt artikel 20 i förordningen tillämpas bara på behandling som grundar sig på samtycke eller avtal. Rätten enligt artikel 21 att göra invändningar mot behandling av uppgifter omfattar bara behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning eller behandling som är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen. Eftersom syftet med behandlingen av personuppgifter enligt 2 kap. 9 § är att utföra polisens lagstadgade uppgifter, tillämpas inte artikel 17, 20 eller 21 på den.

1 §. *Tillgodoseende av den registrerades rätt till insyn.* Enligt paragrafen ska den personuppgiftsansvarige lämna ut behövliga uppgifter och andra uppgifter för utövande av insyn när det är fråga om rätten till insyn enligt 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och den registrerades rätt att få tillgång till uppgifter enligt artikel 15 i dataskyddsförordningen. Den personuppgiftsansvarige kan också förordna någon annan polisenhet att lämna ut uppgifterna. Med avvikelse från nuvarande förfarande kan begäran framföras förutom vid ett personligt besök också via en elektronisk tjänst som tillhandahålls av den personuppgiftsansvarige med hjälp av tillförlitlig elektronisk identifiering.

2 §. *Inskränkningar i rätten till insyn.* I paragrafen föreskrivs om undantag från den registrerades rätt till insyn enligt 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I 1 mom. preciseras de behandlingssyften för vilka rätten ska begränsas. Rätten till insyn gäller inte de personuppgifter som avses i 2 kap. 4 §, observationsuppgifter som avses i 6 § och personuppgifter som avses i 7 § 2 mom. (1 punkten), personuppgifterna om hemlig övervakning och särskild kontroll i Schengens informationssystem (2 punkten), uppgifter om kriminalunderrättelseinhämtning, klassificering eller informationskälla i fråga om en person eller en gärning eller uppgifter som används för brottsanalys och teknisk undersökning av brott (3 punkten) och inte uppgifter som fåtts genom de metoder för inhämtning som avses i 5 kap. i polislagen och 10 kap. i tvångsmedelslagen eller med stöd av 19 kap. 157 § i lagen om tjänster inom elektronisk kommunikation (917/2014) (4 punkten). Till sitt innehåll överensstämmer inskränkningarna i huvudsak med 45 § i gällande lag förutom i fråga om de personuppgifter som avses i 7 § 2 mom., som fogas som nya till 1 punkten och som behandlas för bedömningen av deras nödvändighet. Dessutom ska 3 punkten ändras så att den överensstämmer med de begrepp som används i bestämmelserna om behandlingssyften i 2 kap. Enligt 2 mom. ska registrerade ha rätt att begära att dataskyddsmyndigheten kontrollerar om behandlingen av de personuppgifter som avses i 1 mom. är lagenlig på det sätt som föreskrivs i 29 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Vad gäller behandlingen av personuppgifter som hör till dataskyddsförordningens tillämpningsområde kan den registrerades rätt till insyn enligt 3 mom. inskränkas bara i enskilda fall, om det med beaktande av den registrerades rättigheter är proportionerligt och nödvändigt på de grunder som anges i artikel 23.1 i dataskyddsförordningen. Rätten till insyn kan således begränsas bara utifrån en övervägning i det enskilda fallet, om någon av de grunder som anges i artikel 23.1 föreligger, till exempel i en situation då rätten till insyn är nödvändig för att förhindra brott, och den fördel som uppnåtts med begränsningen kan anses vara så betydande att den ger rätt att begränsa den registrerades rättigheter. Förutom de kriterier som föreskrivs för

behandlingen av personuppgifter annanstans i denna lag, kan det att dataskyddsmyndigheten på begäran av den registrerade får kontrollera att behandlingen av den registrerades personuppgifter är laglig ses som en sådan skyddsåtgärd som avses i artikel 23.2.

3 §. *Utövande av rätten till insyn i den datafil som upprätthålls av den tekniska stödfunktionen i Schengens informationssystem.* Jämfört med tidigare paragrafer innehåller paragrafen en specialbestämmelse om utövande av rätten till insyn. Enligt 1 mom. har var och en rätt att begära att den tillsynsmyndighet som avses i artikel 115 i Schengenkonventionen kontrollerar att insamlingen, registreringen, behandlingen och användningen av personuppgifter som gäller honom eller henne i den datafil som upprätthålls av den tekniska stödfunktionen i Schengens informationssystem sker på ett lagligt och riktigt sätt. Med tillsynsmyndighet avses också i denna paragraf Dataskyddsverket. Den registrerade kan framställa sin begäran om kontroll antingen direkt till dataskyddsmyndigheten eller till en polisinrättning. Polisen ska utan dröjsmål överföra begäran till Dataskyddsverket. Enligt 2 mom. ska en begäran om kontroll framställas personligen hos polisinrättningen, och den som framställer begäran ska samtidigt styrka sin identitet. Paragrafen överensstämmer till sitt innehåll med 47 § i gällande lag.

4 §. *Utövande av rätten till insyn i fråga om behandlingen av personuppgifter som grundar sig på Prümfördraget och Prümrådsbeslutet.* Bestämmelsen överensstämmer med 40 § 3 mom. i gällande lag, men kommer att tas upp i samband med andra bestämmelser om den registrerades rättigheter. Behandlingen av personuppgifter på grundval av Prümfördraget och Prümrådsbeslutet handlar om brottmål, och den registrerade ska ha indirekt rätt till insyn i personuppgifterna genom förmedling av Dataskyddsverket.

7 kap. **Skyddspolisens behandling av personuppgifter**

1 §. *Tillämpningsområde.* På skyddspolisens behandling av personuppgifter tillämpas som allmän lag lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/), om inte något annat föreskrivs i detta kapitel. För skyddspolisens behandling av personuppgifter lämpar sig inte 7 kap. i lagen om behandling av personuppgifter i brottmål, utan i stället tillämpas bestämmelserna i detta kapitel på behandlingen av personuppgifter i internationellt samarbete.

2 §. *Registerföring.* Skyddspolisen för personregister som är knutna till behandlingen av de personuppgifter som avses i detta kapitel.

3 §. *Skyddspolisens behandling av personuppgifter.* Definitionen av skyddspolisens behandling av personuppgifter motsvarar definitionen i 5 § i nuvarande lag om behandling av personuppgifter i polisens verksamhet. Enligt såväl gällande som föreslagna lag får skyddspolisen behandla personuppgifter som är nödvändiga för dess utövande av sitt lagstadgade uppdrag. I samband med lagstiftningen om civil underrättelseinhämtning är avsikten att skyddspolisen fråntas förundersökningsuppgiften och anknytande förundersökningsbefogenheter. I det avseendet bör man beakta att skyddspolisen också när lagstiftningen om civil underrättelseinhämtning har trätt i kraft kommer att ha möjlighet att fungera som expert vid förundersökning av sådana brottshelheter som har betydelse för den nationella säkerheten. I det syftet bör skyddspolisen kunna behandla också personuppgifter med anknytning till undersökningar eller brottsutredningar. I fråga om informationsinnehållet i de personuppgifter som skyddspolisen behandlar hänvisas bland annat till det allmänna innehållet i behandlingen av personuppgifter som är gemensamt med den övriga polisen. Bestämmelser om detta finns i 2 kap. Polisen får behandla personuppgifter som gäller särskilda grupper av personer som definieras i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, och känsliga uppgifter när det är nödvändigt med tanke på skyddspolisens uppdrag. Vad gäller informationsinnehållet görs således inga större ändringar i gällande reglering. Den enda

skillnaden jämfört med gällande lag är regleringen av biometriska uppgifter. Skyddspolisen får redan nu direkt med stöd av lag behandla biometriska uppgifter och den har rätt att ta emot dessa också inom det internationella samarbetet. Därför är det motiverat att behandlingen av uppgifterna regleras också i lagen om personuppgifter.

Dessutom innehåller 4 mom. en informativ hänvisning till lagen om säkerhetsutredningar med stöd av vilken skyddspolisen behandlar också personuppgifter.

4 §. *Behandling av personuppgifter för bedömning av deras betydelse.* Behandlingen av personuppgifter enligt paragrafen för bedömning av deras betydelse överensstämmer med förslaget i 2 kap. 7 § 2 mom. om en bedömning av uppgifternas betydelse.

5 §. *Utlämnande av personuppgifter.* Skyddspolisens uppgift är att inhämta information för att skydda den nationella säkerheten. I detta syfte är det också nödvändigt att lämna ut uppgifter. Personuppgifter ska få lämnas ut till behöriga myndigheter, till sammanslutningar som sköter offentliga uppdrag och i vissa fall också till privata aktörer.

Enligt 1 mom. får skyddspolisen för att utföra sina uppdrag lämna ut uppgifter till andra myndigheter och till sammanslutningar som sköter offentliga uppdrag. I det avseendet görs inga ändringar i gällande lagstiftning.

Enligt 2 mom. får skyddspolisen, liksom övrig polis, lämna ut personuppgifter också för skötseln av andra myndigheters uppdrag. Dessutom får skyddspolisen lämna ut personuppgifter till andra polisenheter när det är nödvändigt för att dessa ska kunna sköta sina uppdrag. I det avseendet ska skyddspolisen även följa vad som föreskrivs om befogenheter. När utlämningen av uppgifter för brottsbekämpning är begränsad enligt bestämmelserna om civil underrättelseinhämtning, ska dessa bestämmelser iakttas. Skyddspolisen får således lämna ut personuppgifter till andra polisenheter för att dessa ska kunna sköta sina uppdrag bara om uppgifterna har inhämtats på annat sätt än genom användning av metoder för underrättelseinhämtning eller om utlämningen av uppgifter inte är begränsad eller förbjuden med stöd av annan lagstiftning.

I 3 mom. föreskrivs om hur personuppgifter ska lämnas ut till privata sammanslutningar eller privatpersoner. Personuppgifter får trots sekretessbestämmelserna i undantagsfall lämnas ut till privata aktörer om det är nödvändigt för att skyddspolisen ska kunna utföra sina uppdrag.

6 §. *Utlämnande av personuppgifter i samband med internationellt samarbete.* I paragrafen föreslås inte några ändringar i gällande reglering av behandlingen av personuppgifter i internationellt samarbete. Skyddspolisens primära uppgift är att bedriva internationellt samarbete med utländska säkerhets- och underrättelsetjänster. I detta syfte får skyddspolisen lämna ut personuppgifter också till utländska behöriga myndigheter. Förutom till utländska säkerhets- och underrättelsetjänster får skyddspolisen lämna ut uppgifter också till andra myndigheter som har som uppgift att trygga den nationella säkerheten, trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet eller förebygga brott, reda ut brott och se till att brott blir föremål för åtalsprövning. Dessutom får skyddspolisen vid behov samarbeta också med internationella brottsbekämpande myndigheter. Skyddspolisen får samarbeta med och lämna ut personuppgifter också till andra internationella myndigheter, såsom Europol och Interpol när myndigheten i fråga har som uppgift att utföra de uppdrag som i paragrafen till

7 §. *Rätt att få information.* Skyddspolisen ska ha samma rätt som polisen att få information om de register och informationssystem som avses i 3 kap. Skyddspolisen ska få information av de instanser och på det sätt som anges i kapitlet och dessutom för att kunna utföra sitt uppdrag, att trygga den internationella säkerheten.

8 §. *Behandling av personuppgifter som fåtts i samband med internationellt samarbete.* Paragrafen motsvarar 31 § i gällande lag. Enligt bestämmelsen ska vid behandlingen av personuppgifter som fåtts från utländska säkerhets- och underrättelsetjänster i fråga om sekretess, tystnadsplikt, begränsningar i användningen av uppgifter, vidareöverlåtelse av uppgifter eller återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna har ställt. Med villkor avses antingen uttryckligen angivna villkor eller vedertagen praxis för dem som är parter i informationsutbytet. I bestämmelsen åläggs inte någon skyldighet att iaktta de villkor som den som har lämnat uppgifterna ställer på förstörande av materialet, utan till denna del tillämpas skyddspolisens egna bestämmelser om förvaringstider för uppgifterna. Begränsningen behövs i synnerhet för att det ska vara möjligt att fastställa informationsutbytets laglighet i sådana fall då det med anledning av att uppgifter erhållits från utlandet även lämnats ut uppgifter från Finland till utlandet.

9 §. *Skyddspolisens rätt att förvalta sitt informationssystem.* Den föreslagna bestämmelsen är ny i förhållande till gällande lag. Syftet med bestämmelsen är att främja skyddet av personuppgifter och säkerställa att de uppgifter som behandlas för att trygga den nationella säkerheten är riktiga och aktuella. Eftersom skyddspolisens informationssystem innehåller uppgifter som behandlas för att trygga den nationella säkerheten är det förenat med särskilda säkerhets- och dataskyddsrisker. För att riskerna ska kunna hanteras har systemet klassificerats högt när det gäller informationssäkerheten, och därför finns det inte några automatiserade förbindelser utåt. Av den anledningen kan inte heller uppgifter uppdateras på samma sätt som i system med en lägre nivå på informationssäkerheten i vilka uppgifter kan uppdateras genom direkta förfrågningar om de registrerade. Det centrala kravet är att uppgifter inte överförs från systemet med den högre säkerhetsnivån till systemet med den lägre säkerhetsnivån i samband med en förfrågan. Därför ska uppgifter i systemet med den högre säkerhetsnivån uppdateras så att det i det mottagande registret inte uppstår några loguppgifter eller andra datamängder som visar vilka uppgifter som har uppdaterats i det informationssystem som upprätthålls för att skydda den nationella säkerheten. Bestämmelsen har ansetts vara nödvändig för att skyddspolisen inte ska äventyra säkerheten för de objekt som är föremål för informationsinhämtning. Enbart uppgifter om att en enskild person är föremål för skyddspolisens inhämtning av information kan utsätta personens eller dennes familjs liv eller hälsa för fara eller påtryckningar i Finland eller utomlands. Å andra sidan kan det äventyra den nationella säkerheten om de objekt eller intressen som är föremål för skyddspolisens informationsinhämtning röjs för utomstående eller för objekten själva.

När uppgifterna jämförs ska större datamängder som samlats in från det utlämnande registret vid en automatisk behandling jämföras med personuppgifterna i skyddspolisens informationssystem. Personregistren kommer inte att vara direkt kopplade till varandra, utan de jämförs på en särskild teknisk plattform. I varje enskilt fall bedöms en tillräckligt stor datamängd. Det kan gälla exempelvis ändrade registeruppgifter, ett visst sampel eller innehållet i hela registret. När bestämmelsen tolkas och tillämpas bör i enskilda fall alltid även de förvaltningsrättsliga principerna beaktas. Bland annat proportionalitetsprincipen förutsätter att ingripanden i en utomståendes rättssfär görs bara i den mån det krävs för att uppnå målet. Med tanke på integritetsskyddet kan den föreslagna bestämmelsen inte ses som någon särskilt viktig utvidgning, eftersom möjligheten att göra jämförelser inte vidgar det informationsinnehåll som skyddspolisen redan nu har rätt till. Bestämmelsen gör lagstiftningen tydligare och mer precis med avseende på skyddspolisens rätt att få nödvändiga personuppgifter för att kunna utföra sina uppdrag och förvalta sina informationssystem med hjälp av en teknisk anslutning eller i form av datamängder, när det är fråga om att uppdatera uppgifter i ett system med hög säkerhetsnivå. Genom bestämmelsen ändras inte lagstiftningens nuvarande läge, men den beaktar de krav som den tekniska utvecklingen ställer på dataskyddet och riktigheten hos personuppgifter som ingår i register.

I 31 § i den föreslagna lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten föreskrivs om skyddet av personuppgifter. Enligt den ska den personuppgiftsansvarige och personuppgiftsbiträdet med tekniska och organisatoriska åtgärder skydda personuppgifter för att säkerställa en nivå på informationssäkerheten som motsvarar risken för en registrerades rättigheter. Personuppgifterna ska särskilt skyddas mot rättsstridig behandling och mot oavsiktlig förlust, förstöring och skada. När åtgärder planeras och genomförs bör man beakta den nyaste tekniken, kostnaderna för genomförandet av åtgärderna, behandlingens art, omfattning, sammanhang och syften samt de risker av varierande sannolikhet och allvarlighetsgrad som riktar sig mot fysiska personers rättigheter.

Enligt 10 § i polisförvaltningslagen (110/1992) har skyddspolisen som uppgift att bekämpa förehavanden och brott som kan äventyra stats- och samhällsskicket eller rikets inre eller yttre säkerhet. Skyddspolisen behandlar således i enlighet med sitt uppdrag uppgifter om de allvarligaste hoten mot Finlands inre och yttre säkerhet och för i detta syfte ett personregister. Med anledning av uppdraget riktas ett ytterst allvarligt hot om olaglig underrättelseverksamhet mot den information som behandlas av skyddspolisen. Med tanke på informationssäkerheten kräver detta effektiva lösningar.

Skyddspolisens informationssystem är uppbyggt för att uppfylla kraven på informationssäkerhet enligt en hög informationssäkerhetsnivå på det sätt som anges i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010). I praktiken innebär detta till exempel att systemet saknar förbindelser utåt. Den föreslagna rätten att granska jämförelseuppgifter har i hög grad att göra med möjligheten att genomföra kraven på informationssäkerhet för uppgifternas del, formellt med att överföra information från ett informationssystem på lägre nivå till ett system på en hög nivå. Alla register ur vilka skyddspolisen har rätt att få uppgifter via en teknisk anslutning, hänförs till en lägre dataskyddsklass.

I 1 mom. i paragrafen kopplas rätten att jämföra uppgifter till lagstadgade rättigheter att få och lämna ut information. I 3 kap. i den föreslagna lagen ingår en förteckning över de med tanke på polisens verksamhet viktigaste registren ur vilka polisen har rätt att få information via en teknisk anslutning eller som en datamängd. Dessutom regleras utlämningen av uppgifter och rätten att öppna en teknisk anslutning i flera andra lagar. I bestämmelsen hänvisas inte särskilt till de register som berörs av rätten att granska jämförelseuppgifter. För tydlighetens skull ska det dock i bestämmelsen upprepas att skyddspolisen trots sekretessbestämmelserna har rätt att få uppgifter som den behöver för att utföra sina uppdrag.

Innan överföringen av uppgifter inleds ska det klarläggas hur nödvändiga jämförelseuppgifter och andra uppgifter tekniskt ska plockas ut ur olika informationssystem och sammanföras i elektronisk form så att informationsinnehållet tillgodoser behoven av jämförelse och så att utplockningen och sammanföringen av uppgifter inte medför onödigt merarbete och onödiga kostnader för den instans som lämnar ut uppgifterna. Samtidigt minimeras behovet av att behandla onödiga uppgifter. Detta tillsammans med skyldigheten att göra en skriftlig konsekvensbedömning framhåller vikten av att behandlingen av personuppgifter är systematisk. Till 32 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten har fogats en bestämmelse om skyddet av personuppgifter vid automatiserad behandling. Den föreslagna bestämmelsen ska tillämpas vid granskningen av jämförelseuppgifter. Med stöd av den säkerställs till exempel att det inte är möjligt att orättmätigt ingripa i automatiserad behandling. Behandlingen av uppgifter ska ordnas så att den effektivt kan övervakas.

I 1 mom. i paragrafen föreskrivs också om skyldigheten att utplåna uppgifter. Efter att jämförelseuppgifterna har analyserats och behandlats ska onödiga jämförelseuppgifter utan dröjsmål utplånas ur skyddspolisens datalager. I praktiken jämförs uppgifterna i en informationssäker

miljö och efter det ska onödiga uppgifter omedelbart utplånas. För tydlighetens skull indelas behandlingen av personuppgifter i paragrafen närmare i olika delar. Med behandling av personuppgifter avses i princip alla åtgärder som gäller behandlingen av uppgifterna. I detta sammanhang behöver det särskilt föreskrivas om tröskeln för att registrera personuppgifter. Syftet med detta är att säkerställa att jämförelsen av uppgifter inte leder till att personer för vilkas del de föreslagna villkoren i 7 kap. 3 § inte uppfylls hamnar i skyddspolisen informationssystem.

Enligt 2 mom. i paragrafen har skyddspolisen rätt att få uppgifterna avgiftsfritt. Arbetet med att plocka ut uppgifter ur informationssystemen och en eventuell anknytande sammanföring kan orsaka kostnader och merarbete för den personuppgiftsansvarige. Avsikten är dock att beakta detta vid begäranden om uppgifter som gäller material och vid begränsningarna av dessa. I praktiken orsakar polisens begäranden om uppgifter alltid merarbete för den som tar emot begäran.

I fråga om tillämpningen av paragrafen bör det dessutom noteras att skyddspolisen ska iaktta den konsekvensbedömning som avses i 20 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Över granskningen av jämförelseuppgifter ska en skriftlig konsekvensbedömning upprättas för dataskyddsmyndigheten som kan vidta åtgärder efter egen prövning. Åtgärderna är enligt lagen till exempel rätten att förbjuda eller avbryta behandlingen av uppgifter. Syftet med detta är att säkerställa att behandlingen av personuppgifter följer de allmänna principerna för behandling av uppgifter, exempelvis proportionalitetsprincipen. Om förfarandet enligt planerna ska upprepas med samma innehåll, behöver den skriftliga konsekvensbedömningen göras bara en gång.

I 19 § i den föreslagna lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten föreskrivs det om logguppgifter. Den personuppgiftsansvarige och personuppgiftsbiträdet ska se till att loggar förs över följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning, överföring, sammanförande och radering av personuppgifter. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för händelsen samt uppgifter om vem som har läst eller lämnat ut personuppgifter samt om möjligt om vilka som har fått tillgång till personuppgifterna. Loggarna får användas bara för kontroll av behandlingens laglighet, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet samt inom ramen för straffrättsliga förfaranden. Informationssystemet ska vara underställd ett heltäckande loggsystem för att möjliggöra en effektiv laglighetsövervakning av systemet. Den rättsliga grunden för varje utlämning av uppgifter ska kunna kontrolleras också i efterhand.

10 §. *Inskränkningar i rätten till insyn.* Bestämmelsen överensstämmer med 45 § i gällande lag. Inskränkningarna i rätten till insyn inbegriper också uppgifter som behandlats med tanke på bedömningen av deras betydelse. I lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten föreskrivs om uppgifterna på lagens tillämpningsområde för den dataskyddsmyndighet som ersätter dataombudsmannen. I paragrafen föreskrivs därför att indirekt rätt till insyn kan utövas via dataskyddsmyndigheten på det sätt som avses i 29 § i lagen i fråga.

11 §. *Utplåning av uppgifter. Regleringen överensstämmer med 25 § i gällande lag.* Som en ny bestämmelse i lagen införs möjligheten att bevara uppgifter i över 25 år, om det finns särskilda skäl att bevara dem för att skyddspolisen ska kunna utföra sina uppdrag. Lagen ska utökas med en skyldighet att bedöma uppgifternas nödvändighet och grunden för behandlingen vart femte år om uppgifterna behöver bevaras över den maxtid som föreskrivs i lagen. Om det konstateras att det fortfarande är nödvändigt att bevara uppgifterna, ska det i samband med uppgifterna göras en anteckning om bedömningen (1 mom.).

Enligt 2 mom. får dessutom uppgifterna om den bedömning av betydelse som avses i 4 § bevaras i sex månader. I det avseendet är det inte längre nödvändigt att särskilt föreskriva om en bedömning av om det fortfarande finns ett behov av att bevara uppgifterna, eftersom förfarandet redan från första början gällde bedömningen av om uppgifterna är nödvändiga för skyddspolisens behandlingssyften. Uppgifterna ska utplånas genast när det står klart att de inte längre är av betydelse för avsett behandlingssyfte.

12 §. *Arkivering av uppgifter.* Paragrafen innehåller en informativ hänvisning till arkivering av uppgifter enligt arkivlagen.

8 kap. **Särskilda bestämmelser**

1 §. *Skydd av känsliga personuppgifter.* I EU:s nya dataskyddslagstiftning ställs särskilda krav på skyddet av känsliga personuppgifter. Enligt artikel 29.1 i direktivet ska medlemsstaterna föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheteter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller de särskilda kategorier av personuppgifter som avses i artikel 10. Med särskilda kategorier av personuppgifter avses känsliga uppgifter. I fråga om den behandling som hör till direktivets tillämpningsområde kompletterar paragrafen bestämmelserna om informationssäkerhet i 5 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Krav på säker behandling ställs också i dataskyddsförordningen. I artikel 32.1 i förordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Kraven i artikel 32 i förordningen gäller behandlingen av såväl känsliga uppgifter som andra personuppgifter, och kraven tillämpas med stöd av förordningen direkt även på polisen som personuppgiftsansvarig. De mer detaljerade krav som i paragrafen ställs på behandlingen av känsliga uppgifter är, när det gäller de uppgifter som hör till förordningens tillämpningsområde, de specifika krav som fastställs i artikel 6.2 för att säkerställa en laglig och rättvis behandling. De specifika krav som ställs på informationssäkerheten inbegriper samtidigt de bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen som förutsätts i artikel 9.2 g i förordningen.

Polisens behov av att behandla känsliga uppgifter är ofta kopplat till syftet med behandlingen. Till exempel biometriska uppgifter behandlas i samband med brottmål, tillståndsärenden och utlänningsärenden. Vidare används såväl biometriska uppgifter (fingeravtryck) som genetisk information (DNA-spår) för identifiering av brottsmisstänkta, också i sådana informationssystem som möjliggör en omfattande behandling och sökning av personuppgifter i en annan medlemsstats system. För skötseln av sina uppdrag behandlar polisen förutom biometriska och genetiska uppgifter också andra känsliga uppgifter, såsom uppgifter om hälsotillstånd. Syftet med 1 mom. i den föreslagna paragrafen är att säkerställa att de specifika garantier för skyddet av personuppgifter och informationssäkerhet som ställs i dataskyddsförordningen och dataskyddsdirektivet iakttas. I den ställs specifika krav på informationssäkerhet vid registrering och annan behandling av dessa identifierare.

I 2 mom. i paragrafen ställs mer detaljerade krav på vad som behöver beaktas vid registrering och annan behandling av känsliga personuppgifter. Kraven gäller såväl informationssystem, anordningar och programvaror som skydd mot obehörig åtkomst till uppgifter och uppgifternas konfidentialitet och integritet. Dessutom förutsätts särskilda tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter kan genomföras informationssäkert och på ett sätt som tryggar integritetsskyddet. Enligt 3 mom. i paragrafen gäller den personuppgiftsansvariges skyldigheter också i relation till tredje parter som helt eller delvis sköter registreringen av känsliga uppgifter. Detta innebär att man i ett uppdragsavtal ska försäkra sig om att en tredje part har samma skyldighet att skydda känsliga uppgifter och att denne i annat fall inte skulle ha rätt att behandla uppgifterna.

2 §. *Personuppgiftsansvarig.* I paragrafen preciseras vilken enhet vid polisen som ska svara för registerföringen av de personuppgifter som behandlas för syften som föreskrivs i 2 kap. Eftersom det i propositionen inte ingår några förslag till bestämmelser om att inrätta personregister som kan användas av en eller flera polisenheter enligt 6 § 2 mom. i gällande lag, föreslås det att Polisstyrelsen ska vara personuppgiftsansvarig för alla personuppgifter som behandlas för de syften som anges i 2 kap. Skyddspolisen föreslås vara personuppgiftsansvarig för de personuppgifter som avses i 7 kap. Registerföringen av registret för förhindrande, avslöjande och utredning av penningtvätt och av finansiering av terrorism, penningtvättsregistret, regleras särskilt i lagen om centralen för utredning av penningtvätt. Till denna del berörs Centralkriminalpolisen av alla de skyldigheter som den personuppgiftsansvarige har enligt lagförslaget. Bestämmelser om registerföringen av passageraruppgifter finns i lagförslag 2.

3 §. *Skyddsåtgärder i civilrättsliga frågor.* Paragrafen överensstämmer till sitt innehåll med 47a § i gällande lag. Enligt den ska det som i denna lag föreskrivs om behandlingen av personuppgifter som gäller besöksförbud tillämpas på skyddsåtgärder som anmälts till polisens register med stöd av 4 § i lagen om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor (227/2015).

4 §. *Närmare bestämmelser och anvisningar.* I 1 mom. i paragrafen ges statsrådet bemyndigande att utfärda förordning. Med stöd av det får närmare bestämmelser om förfaringssätt vid beslut om utlämnande av personuppgifter enligt 4 kap. 10 § och vid utövande av rätt till insyn enligt 8 kap. 2 § utfärdas genom förordning av statsrådet. Enligt 2 mom. fastställer Polisstyrelsen formulären för de blanketter som ska användas vid åtgärder som hör till polisen, om inte något annat föreskrivs i lag. Paragrafen överensstämmer med 48 § i gällande lag, med undantag för bestämmelsen om anvisningar.

5 §. *Ikraftträdande.* I paragrafen föreskrivs om lagens ikraftträdande. Lagen avses träda i kraft den 2018 och genom den upphävs lagen av den 1 oktober 2003 om behandling av personuppgifter i polisens verksamhet (761/2003). Den personuppgiftsansvarige får vidta åtgärder som verkställigheten av lagen förutsätter innan lagen träder i kraft.

1.2 Lag om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet

Lagförslaget är nytt och grundar sig på Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (EU:s PNR-direktiv). Direktivet förpliktar lufttrafikföretag att överföra fastställda PNR-uppgifter till de enheter för passagerarinformation som inrättats eller utsetts av medlemsstaterna för analys av uppgifterna

samt från enheten för eventuell överföring till behöriga myndigheter, en enhet för passagerarinformation i en annan medlemsstat eller till Europol för bedömning av om det behövs utredningar för att dessa ska kunna identifiera personer som är delaktiga i sådana terroristbrott eller sådan grov brottslighet som definieras i direktivet. Medlemsstaterna ska genomföra direktivet senast den 25 maj 2018.

1 §. *Tillämpningsområde.* Enligt paragrafen genomförs genom denna lag Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, nedan PNR-direktivet.

2 §. *Förhållande till annan lagstiftning.* I paragrafen preciseras lagförslagets förhållande till annan lagstiftning. Förutom lagförslaget tillämpas också lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/2018) på behandlingen av passageraruppgiftssamlingar vid en enhet för passagerarinformation. Lagförslaget syftar till att genomföra

Europaparlamentets och rådets direktiv (EU) 2016/680 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 (dataskyddsdirektivet). Den föreslagna lagen är en speciallag som ska komplettera lagstiftningen i fråga.

3 §. *Definitioner.* I paragrafen ingår de definitioner som ska användas i lagen. I bestämmelsen definieras lufttrafikföretag (1 punkten), flygning utanför Europeiska unionen (2 punkten), flygning inom Europeiska unionen (3 punkten), passagerare (4 punkten), passageraruppgiftssamling (PNR, Passenger Name Record) (5 punkten), reservationssystem (6 punkten), terroristbrott (7 punkten), grov brottslighet (8 punkten), maskering (9 punkten), behöriga myndigheter (10 punkten) och Europol (11 punkten). Definitionerna i 1–9 punkten överensstämmer med definitionerna i artikel 3 i PNR-direktivet. Med terroristbrott (7 punkten) avses terroristbrott enligt 34 a kap. 1–5 § i strafflagen (1889/33), medräknat olika brott som begåtts i terroristiskt syfte, förberedelse till brott som begås i terroristiskt syfte, ledning av terroristgrupper, främjande av terroristgruppers verksamhet och finansiering av terrorism. I PNR-direktivet hänvisas i fråga om terroristbrott till rådets rambeslut 2002/475/RIF (artikel 1–4) som har ersatts med Europaparlamentets och rådets direktiv (EU) 2017/541, terrorismdirektivet) om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF. Enligt artikel 27 i terrorismdirektivet ska hänvisningar till rambeslut 2002/475/RIF anses som hänvisningar till detta direktiv. Den skyldighet som åläggs i terrorismdirektivet att kriminalisera terroristbrott är betydligt mer omfattanden än skyldigheten enligt artikel 1–4 i rambeslutet. Nya kriminaliseringsförpliktelser är bland annat offentlig uppmaning till terroristbrott, rekrytering av terrorister, tillhandahållande och mottagande av utbildning för terrorismsyften, resor för terrorismsyften, organisering eller annat underlättande av resor för terrorismsyften samt finansiering av terrorism i vidare mening än tidigare. Medlemsstaterna ska införliva terrorismdirektivet med den nationella lagstiftningen senast den 8 september 2018. Med grov brottslighet i 8 punkten avses brott som förtecknas i bilaga II till PNR-direktivet och vilka bestraffas med fängelse eller annan frihetsberövande åtgärd eller säkringsåtgärd i minst tre år enligt medlemsstatens nationella rätt. Beträffande grov brottslighet innehåller bilaga II till PNR-direktivet en brottsförteckning med 26 punkter, till exempel deltagande i en kriminell organisation, människohandel, it-brottslighet/cyberbrottslighet och kapning av flygplan eller fartyg. Behöriga myndigheter i Finland enligt punkt 10 i PNR-direktivet är polisen, Tullen och Gränsbevakningsväsendet.

4 §. *Lufttrafikföretags skyldighet att överföra passageraruppgifter.* Enligt 1 mom. i paragrafen ska ett lufttrafikföretag överföra passageraruppgifter enligt denna paragraf för såväl ankommande som avgående flygningar utanför eller inom Europeiska unionen som de utför, till den del uppgifterna har samlats in som en del av den normala affärsverksamheten. I fråga om flygningar med gemensam linjebeteckning gäller skyldigheten det företag som utför flygningen. Passageraruppgifterna ska överföras till den enhet för passagerarinformation som avses i 5 §. Om lufttrafikföretaget också har samlat in sådan förhandsinformation om passagerare som avses i punkt 18 i bilaga I till PNR-direktivet, ska även denna information överföras. Lufttrafikföretaget ska överföra passageraruppgifterna avgiftsfritt.

I artikel 8.1 i PNR-direktivet fastställs lufttrafikföretags skyldighet att överföra passageraruppgifter till enheten för passagerarinformation och i artikel 8.2 anges medlemsstaternas skyldighet att se till att lufttrafikföretagen överför också den förhandsinformation om passagerare, s.k. API-uppgifter (Advance Passenger Information), som avses i punkt 18 i bilaga I. Av artikel 2 i PNR-direktivet framgår att en medlemsstat kan tillämpa PNR-direktivet också på flygningar inom EU, antingen på alla eller bara på valda flygningar. Enligt 3 kap. 13 § 1 mom. 16 punkten i lagen om behandling av personuppgifter i polisens verksamhet (761/2003) har polisen redan rätt att av samfund och sammanslutningar få uppgifter ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott, för överlämnande till åtalsprövning samt för att nå efterlysta personer. Den gällande bestämmelsen gäller dock bara enskilda fall. Lufttrafikföretag ska som regel överföra de uppgifter som avses i 1 mom. i den föreslagna paragrafen för alla ankommande och avgående flygningar utanför eller inom Europeiska unionen. Uppgifterna ska överföras avgiftsfritt. Genom det föreslagna 1 mom. genomförs artikel 2 i PNR-direktivet samt artikel 8.1 delvis och artikel 8.2.

Enligt 2 mom. i paragrafen är de passageraruppgifter som avses ovan i 1 mom. följande: 1) PNR-nummerkod, 2) datum för bokning/utfärdande av biljett, 3) datum för avsedd resa, 4) namn, 5) adress och kontaktuppgifter, 6) all tillgänglig betalningsinformation, också faktureringsadress, 7) hela reserutten för en specifik bokning, 8) uppgifter om bonusprogram, 9) resebyrå/resebyråtjänsteman, 10) passagerares resestatus inklusive bekräftelser och incheckningsstatus, passagerare som inte har checkat in eller passagerare som checkat in utan bokning, 11) delade PNR-uppgifter, 12) allmänna anmärkningar (inklusive all tillgänglig information om minderåriga under 18 år utan medföljande vårdnadshavare, såsom den minderåriges namn och kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som ledsagar barnet vid avresan samt uppgifter om personens relation till den minderårige, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet samt uppgifter om personens relation till den minderårige, flygplatsanställd som ledsagar barnet vid avresan respektive ankomsten), 13) biljettinformation, inbegripet biljettnummer, datum för utfärdande av biljetten, enkelbiljetter och automatisk biljettprisuppgift (ATFQ, Automated Ticket Fare Quote), 14) platsnummer och annan platsinformation, 15) information om gemensam linjebeteckning, 16) all bagageinformation, 17) antal medresenärer, och deras namn, i samband med en bokning, 18) eventuell förhandsinformation om passagerare (Advance Passenger Information, API) om sådan har samlats in, 19) alla ändringar som gjorts av de PNR-uppgifter som anges i nummer 1–18. Genom det föreslagna 2 mom. genomförs skyldigheten enligt artikel 8.1 i PNR-direktivet att överföra uppgifterna i direktivets bilaga I.

Enligt 3 mom. ska passageraruppgifterna överföras 24 timmar före den planerade ankomst- eller avgångstiden för flygningen och omedelbart efter det att gatens dörrar stängts, varvid överföringen av uppgifter också kan begränsas till uppdateringar av tidigare överföringar. Om uppgifterna behövs för att man ska kunna reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska uppgifterna på begäran av enheten för passagerarinformation överföras även vid andra tidpunkter. Enligt artikel 8.3 a i PNR-direktivet

ska uppgifterna överföras 24-48 timmar före flygningens planerade avgång, och enligt punkt 3 b omedelbart efter det att gatens dörrar har stängts. När enheten för passagerarinformation byggdes upp sågs 24 timmar som en lämplig tid. Beträffande tiden skulle det vara ändamålsenligt att alla medlemsstater följde samma praxis, saken diskuteras för närvarande av medlemsstaterna och kommissionen. Enligt artikel 8.4 ska medlemsstaterna tillåta lufttrafikföretag att begränsa den överföring som avses i punkt 3 b till uppdateringar av sådana överföringar som avses i punkt 3 a. I situationer där åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska enligt artikel 8.5 lufttrafikföretag efter en bedömning i det enskilda fallet på begäran av en enhet för passagerarinformation, i enlighet med nationell rätt, överföra PNR-uppgifter vid andra tidpunkter än de som anges i punkt 3. Genom det föreslagna 3 mom. genomförs artikel 8.3–5 i PNR-direktivet.

I 4 mom. i paragrafen föreskrivs dessutom om skyldigheten att vid överföring av passageraruppgifter använda de i artikel 16 i PNR-direktivet avsedda gemensamma protokoll och understödda dataformat som antagits genom kommissionens genomförandeakt. Kommissionens första genomförandeakt antogs den 26 april 2017 (EUT L 113, 29.4.2017). Genom det föreslagna 4 mom. genomförs artikel 8.3, första stycket och artikel 16.2 och 16.3.

5 §. *Enhet för passagerarinformation.* I paragrafen preciseras den enhet för passagerarinformation som avses i lagen och som utgörs av en sådan riksomfattande PTG-underrättelseenhet som avses i 5 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009). Artikel 4 i PNR-direktivet ålägger varje medlemsstat att inrätta eller utse en myndighet med behörighet att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet eller en avdelning inom en sådan myndighet, vilken ska fungera som medlemsstatens enhet för passagerarinformation. I Finland är den riksomfattande PTG-kriminalunderrättelseenhet som avses i 5 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet(687/2009) en sådan enhet för passagerarinformation som avses i direktivet. Vid enheten arbetar företrädare för polisen, Tullen och Gränsbevakningsväsendet som är de behöriga myndigheter som förutsätts i PNR-direktivet. I avsnitt 4.3, konsekvenser för myndigheterna, i stycket om PNR-direktivet i den allmänna motiveringen till lagförslag 1 i propositionen, ingår en närmare beskrivning av enheten för passagerarinformation och dess verksamhet. I propositionen ingår också ett förslag till ändring av 5 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet genom vilken den riksomfattande PTG-kriminalunderrättelseenheten fastställs som permanent. I samband med det stryks hänvisningen till särskilda polisbefogenheter i den sista meningen i det gällande 1 mom. i 8 § i den upphävda polislagen (493/1995). Bestämmelser om särskilda polisbefogenheter ingår inte i gällande polislag. Dessutom är det lämpligt att ändra 3 § i statsrådets förordning om samarbete mellan polisen, tullen och gränsbevakningsväsendet (1126/2009) så att polisöverdirektören, generaldirektören för Tullstyrelsen och chefen för gränsbevakningsväsendet beslutar i den riksomfattande PTG-ledningsgruppen om de riksomfattande PTG- kriminalunderrättelseenheternas närmare uppbyggnad samt om inrättande och indrag av enheterna. Genom den föreslagna 5 § och ändringarna av PTG-lagen och PTG-förordningen genomförs PNR-direktivets artikel 4.

6 §. *Behandling av passageraruppgifter.* Enligt 1 mom. i paragrafen får enheten för passagerarinformation behandla passageraruppgifter för identifiering av personer som kan vara delaktiga i terroristbrott eller grov brottslighet, enligt följande: 1) före passagerarnas beräknade ankomst eller avresa, 2) på motiverad begäran, som bygger på tillräckliga observationer, från de behöriga myndigheterna, enheten för passagerarinformation i en annan medlemsstat eller Europol, och 3) i enlighet med på förhand fastställda kriterier för bedömning och analys eller för att uppdatera kriterierna eller fastställa nya kriterier.

Enligt artikel 6.2 a i PNR-direktivet får enheten för passagerarinformation behandla PNR-uppgifter för att göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten. Genom förslaget i 6 § 1 mom. 1 punkten genomförs artikel 6.2 a i PNR-direktivet.

Enligt artikel 6.2 b i PNR-direktivet får enheten för passagerarinformation behandla PNR-uppgifter genom att i enskilda fall besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol resultaten av sådan behandling. Enligt artikel 9.2 i PNR-direktivet har en medlemsstat rätt att vid behov begära PNR-uppgifter från enheten för passagerarinformation i vilken medlemsstat som helst. Enligt artikel 10.1 i PNR-direktivet har Europol rätt att inom ramen för sina befogenheter och för fullgörandet av sina arbetsuppgifter begära PNR-uppgifter eller resultatet av behandlingen av dessa uppgifter från enheterna för passagerarinformation i medlemsstaterna. Genom förslaget i 1 mom. 2 punkten genomförs artikel 6.2 b och artikel 9.2 samt artikel 10.1 i PNR-direktivet.

Enligt artikel 6.2 c i PNR-direktivet får enheten för passagerarinformation analysera PNR-uppgifter för att uppdatera och skapa nya kriterier och enligt 3b behandla PNR-uppgifter i enlighet med på förhand fastställda kriterier. Genom förslaget i 1 mom. 3 punkten genomförs artikel 6.2 c och 6.3 b i PNR-direktivet.

Inom brottsbekämpningen kan passagerarinformation användas på många olika sätt. Först och främst kan informationen användas reaktivt: i samband med brottsutredningar, lagföring eller upplösning av kriminella nätverk efter det att ett brott redan har begåtts. För att de brottsbekämpande myndigheterna ska få tillgång till de gamla uppgifter som de behöver måste de ha rätt att lagra uppgifterna tillräckligt länge. Informationen kan användas också i realtid, innan en passagerare har anlänt eller avrest, i syfte att förhindra ett brott, övervaka eller gripa personer innan ett brott har begåtts eller på grund av att ett brott har begåtts eller håller på att begås. I dessa fall behövs PNR-uppgifter för en jämförelse mot redan fastställda bedömningskriterier vilket gör det möjligt att identifiera tidigare okända misstänkta, eller för att söka i olika databaser över eftersökta personer och föremål. Vidare kan uppgifterna användas proaktivt för analys och för att skapa bedömningskriterier som sedan kan användas för bedömning av passagerare före ankomst och avresa. För att de brottsbekämpande myndigheterna ska ha nytta av en sådan analys för att förebygga, upptäcka, utreda och lagföra terroristbrott och grov brottslighet måste de ha rätt att lagra uppgifterna tillräckligt länge. Proaktiv användning av uppgifter är till exempel att man kommer eventuella terrorister eller kriminella grupper som smugglar droger eller bedriver människohandel på spåren genom att analysera sätten att resa och tillvägagångssätt som avviker från det normala. Som avvikande kan nämnas till exempel kontantbetalning för bokningar som gjorts i sista minuten eller att en passagerare saknar bagage. Avsikten kan vara att dölja en passagerares identitet. Flygning är ett snabbt, enkelt och billigt sätt att resa också för den som planerar terroristiska gärningar. Nyttan av analyser av passagerarinformation vid brottsbekämpning kan jämföras med analyser av routning och dess innehåll i samband med telekommunikation. Trots att det är allmänt känt, också bland dem som planerar brott, att myndigheterna har möjlighet att, antingen i realtid eller i efterhand, analysera telekommunikationen, har teleövervakning ändå stor betydelse som ett arbetsredskap för brottsbekämpande myndigheter.

Enligt 2 mom. i paragrafen ska de i 1 mom. 3 punkten avsedda bedömningskriterierna, som enheten för passagerarinformation fastställer och i samarbete med de behöriga myndigheterna regelbundet ser över, vara riktade, proportionella och tydliga. Bedömningskriterierna får inte grunda sig på uppgifter om en persons ras, etniska ursprung, politiska åskådning, religiösa el-

ler filosofiska övertygelse, medlemskap i fackförbund, hälsotillstånd, sexualliv eller sexuella läggning. Genom den föreslagna bestämmelsen i 2 mom. genomförs artikel 6.4 i PNR-direktivet. Genom momentet uppfyller medlemsstaterna samtidigt skyldigheten enligt artikel 11.3 i PNR-direktivet att förvissa sig om att profilering inte leder till diskriminering. Medlemsstaterna ska se till att kriterierna fastställs och regelbundet ses över av enheterna för passagerarinformation i samarbete med de behöriga myndigheter som avses i artikel 7. Dessa på förhand fastställda kriterier får under inga omständigheter vara baserade på en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.

I 3 mom. i paragrafen föreskrivs om rätten för enheten för passagerarinformation att i samband med den behandling som avses i 1 mom. 1 punkten genom automatiserade metoder jämföra passageraruppgifter med 1) uppgifter som lagrats i syfte att trygga de behöriga myndigheternas brottsutredning och kriminalunderrättelseinhämtning samt rätts- och samhällsordningen och att upprätthålla allmän ordning och säkerhet, 2) de personuppgifter som avses i 7 kap. 3 § i lagen om behandling av personuppgifter i polisens verksamhet (/) och som behandlas av skyddspolisen, samt 3) de uppgifter som lagrats i det i 1 kap. 3 § 2 punkten i lagen om behandling av personuppgifter i polisens verksamhet avsedda Schengens informationssystems och den internationella kriminalpolisorganisationens (ICPO-Interpol) databaser.

Enligt artikel 6.3 a i PNR-direktivet får enheten för passagerarinformation jämföra PNR-uppgifter med uppgifter i databaser som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inklusive databaser över personer eller föremål som är eftersökta eller finns uppförda på spärrlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser. I 2 kap. i lagförslag 1 i propositionen föreskrivs närmare om behandlingen av personuppgifter i polisens verksamhet. I den föreslagna 2 kap. 3 § föreslås bestämmelser om behandling av personuppgifter i utredningssyfte, i 4 § om behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning och i 5 § om behandling av personuppgifter för upprätthållande av allmän ordning och säkerhet. I 7 kap. 3 § i lagförslaget föreskrivs närmare om skyddspolisens rätt att behandla personuppgifter som är nödvändiga för att trygga den nationella säkerheten samt rätts- och samhällsordningen eller för att förhindra, avslöja och utreda verksamheter, projekt och brott som hotar landets säkerhet.

För Gränsbevakningsväsendets del blir det i första hand fråga om behandling av personuppgifter i utredningssyfte samt behandling av personuppgifter för kriminalunderrättelseinhämtningens syften. Regleringen som gäller utredningssyften inbegriper behandling av personuppgifter med anknytning till Gränsbevakningsväsendets förundersökningar och annan brottsbekämpning, och regleringen som gäller kriminalunderrättelseinhämtningens syften avser behandling av personuppgifter med anknytning till Gränsbevakningsväsendets inhämtning och analys av kriminalunderrättelser. För Tullens del är det först och främst fråga om behandling av personuppgifter i utredningssyfte samt behandling av personuppgifter för kriminalunderrättelseinhämtningens syften. För närvarande finns det inte några planer på att revidera lagstiftningen om behandlingen av personuppgifter för någondera myndighetens del.

Som databaser som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet kan också anses de uppgifter som lagrats i det i 1 kap. 3 § 2 punkten i lagförslag 1 till lag om behandling av personuppgifter i polisens verksamhet avsedda Schengens informationssystems och den internationella kriminalpolisorganisationens (ICPO-Interpol) databaser.

Genom förslagen i 3 mom. 1–3 punkten genomförs artikel 6.3 a i PNR-direktivet.

Enligt artikel 7.4 i PNR-direktivet får PNR-uppgifter och resultaten av behandlingen av dessa uppgifter som mottas av enheten för passagerarinformation vidarebehandlas av de behöriga myndigheterna i medlemsstaterna bara för specifika syften, såsom att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. Enligt artikel 7.5 i direktivet ska punkt 4 inte påverka de brottsbekämpande eller rättsliga myndigheternas befogenheter på nationell nivå, om andra brott eller indikationer på sådana upptäcks i samband med brottsbekämpande insatser som görs till följd av sådan behandling av PNR-uppgifter. Om specifika PNR-uppgifter har överförts till en behörig myndighet för att användas inom ramen för särskilda brottsutredningar eller lagföringsåtgärder, bör enligt skäl 26 i ingressen den behöriga myndighetens lagring av dessa uppgifter regleras av nationell rätt, oavsett vilken lagringstid för uppgifter som anges i detta direktiv. Vid behandling av PNR-uppgifter eller resultat av behandlingen av uppgifterna som erhållits från enheten för passagerarinformation för bekämpning av terrorism och grov brottslighet, får polisen, Tullen och Gränsbevakningsväsendet behandla uppgifterna också för bekämpning av annan brottslighet, om det till följd av behandlingen framkommer andra brott eller indikationer på sådana.

PNR-direktivet och förslaget till lag om genomförande av direktivet kommer inte att begränsa rätten att få information eller behandlingen av uppgifter som grundar sig på annan lagstiftning och inte heller utbytet av uppgifter om passagerare i utrikestrafiken. Sådan reglering ingår åtminstone i lagen om behandling av personuppgifter i polisens verksamhet, lagen om behandling av personuppgifter vid gränsbevakningsväsendet och lagen om behandling av personuppgifter inom Tullen. PNR-direktivet och lagen om genomförande av direktivet ålägger transportörer en ny skyldighet att lämna ut uppgifter. För att den nya lagstiftningen inte i onödan ska öka transportörernas administrativa börda, bör de myndigheter som behöver passagerarinformation i första hand enas om möjligheten att ta emot dessa uppgifter som lämnats ut med stöd av olika lagstiftningar via en enda kanal och eventuellt rentav vid ett och samma tillfälle. Dessutom bör myndigheterna enas om hur de uppgifter som lämnats ut och tagits emot ska vidarefördelas till de nationella behöriga myndigheterna.

Enligt 4 mom. i paragrafen ska eventuella träffar i samband med sådan behandling av passageraruppgifter som avses i 1 mom. 1 punkten granskas individuellt. Enligt artikel 6.5 i PNR-direktivet ska medlemsstaterna se till att eventuella träffar i samband med automatisk behandling av PNR-uppgifter enligt punkt 2 a (bedömning av passagerare före deras beräknade ankomst eller avresa) granskas individuellt med icke-automatiska metoder, för att verifiera huruvida den behöriga myndighet som avses i artikel 7 behöver vidta åtgärder enligt nationell rätt. Genom det föreslagna 4 mom. genomförs artikel 6.5 i PNR-direktivet.

Enligt 5 mom. ska jämförelse enligt 3 mom. 2 punkten genomföras på ett sätt som tryggar dataskyddet, i enlighet med vad som avtalas med den personuppgiftsansvarige. Momentet gäller en jämförelse av PNR-uppgifter med de personuppgifter som behandlas av skyddspolisen. Genom förslaget i momentet framhålls kraven på dataskydd som uppstår när uppgifter behandlas i ett informationssystem med hög datasäkerhet (skyddsnivå II).

Enligt 14 § i förslaget till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska den personuppgiftsansvarige svara för att personuppgifter behandlas lagenligt. Enligt 15 § i samma lagförslag ska den personuppgiftsansvarige när metoder för behandlingen av personuppgifter fastställs och i samband med behandlingen av uppgifterna vidta lämpliga tekniska och organisatoriska skyddsåtgärder för att förvissa sig om att behandlingen är lagenlig och den registrerades rättigheter tryggas. När åtgärderna genomförs ska de tekniska lösningar som står till förfogande, kostnaderna för åtgärderna samt behandlingens art, omfattning, sammanhang och syften beaktas liksom de risker som riktar sig mot fysiska personers rättigheter. Enligt 31 § i lagförslaget ska den personuppgiftsansvarige och personuppgiftsbiträdet genom tekniska och organisatoriska åtgärder skydda personuppgif-

terna för att förvissa sig om en säkerhetsnivå som är lämplig i förhållande till risken för den registrerades rättigheter. Bestämmelser om skyddet av personuppgifter finns också i PNR-direktivet. Enligt artikel 13.7 direktivet ska medlemsstaterna se till att deras enhet för passagerarinformation genomför lämpliga tekniska och organisatoriska åtgärder och förfaranden för att säkerställa en så hög säkerhetsnivå som är lämplig med tanke på de risker som är förknippade med behandlingen och arten av PNR-uppgifterna.

Den föreslagna bestämmelsen kan anses ha en delvis informativ karaktär, eftersom bestämmelserna ovan förutsätter att all behandling av personuppgifter genomförs på ett sätt som tryggar dataskyddet. Bestämmelser om dataskydd ingår också i gällande lagstiftning om behandling av personuppgifter. Förslaget till bestämmelse ses dock som nödvändigt, eftersom jämförelsen görs i ett informationssystem på skyddsnivå II, vilket vid informationsbehandlingen kräver avvikande tekniker med ett starkare skydd jämfört med andra system på lägre datasäkerhetsnivå. I det avseendet är det lämpligt att framhålla vikten av att jämförelsen görs på ett datasäkert sätt, eftersom man blir tvungen att tillgripa metoder som avviker från andra informationssystem på en lägre säkerhetsnivå.

Enligt 5 mom. får jämförelsen genomföras bara av en tjänsteman som skyddspolisen förordnat till uppgiften vid enheten för passagerarinformation. Redan tidigare i lagstiftningen har man omfattat ståndpunkten att utomstående inte ska ha åtkomst till skyddspolisens informationssystem på grund av att innehållet är känsligt. Saken har beskrivits på följande sätt i tidigare förarbeten till lagen om behandling av personuppgifter i polisens verksamhet: ”Datasystemet är avsett att användas av en enda polisenhet, nämligen skyddspolisen, varför endast personer som hör till skyddspolisens personal skall ha rätt att använda det” (RP 39/1994 s.15).

Det föreslagna momentet anknyter också till de krav på datasäkerhet som behandlas ovan. I praktiken innebär bestämmelsen en skyldighet att begränsa behandlingen av uppgifter med organisatoriska medel, eftersom bara en avgränsad grupp av användare kan ges åtkomst till hemligt eller särskilt känsligt faktamaterial. I skyddspolisens register är det dessutom även möjligt att registrera personer vilkas delaktighet i handlingar som skyddas genom direktivet kan vara i viss mån mer diffus eller osäker än i andra liknande personregister som ingår i jämförelsen. Därför krävs kännedom om polisens verksamhetsområde hos den som ska bedöma om uppgifterna är i den mån väsentliga och nödvändiga att de behöver lämnas vidare till behöriga myndigheter, andra enheter för passagerarinformation, Europol eller ett tredje land. Enligt sista meningen i 5 mom. kan de passageraruppgifter som observerats genom jämförelsen enligt 6 § 3 mom. 2 punkten och resultaten av behandlingen av uppgifterna vidarebefordras bara med samtycke av skyddspolisen.

Enligt skäl 23 i ingressen till PNR-direktivet får bestämmelserna i detta direktiv inte påverka andra unionsinstrument om informationsutbyte mellan polismyndigheter och andra brottsbekämpande myndigheter och rättsliga myndigheter. Till unionsakterna hör också fördraget om Europeiska unionen (EU-fördraget). I artikel 4.2 i fördraget framhävs uttryckligen att den nationella säkerheten är varje medlemsstats eget ansvar. Till skyddspolisens uppgifter hör att upprätthålla den nationella säkerheten, och därför omfattas dess verksamhet inte av tillämpningsområdet för unionsrätten.

Även om det är skyddspolisens uppgift att upprätthålla den nationella säkerheten, är skyddspolisen samtidigt också till sin karaktär en polismyndighet. I Finland hör det till dess ansvarsområde att förhindra och avslöja terrorism samt administrera ett informationssystem i vilket tillhörande personuppgifter kan registreras. Om det inte vore möjligt att jämföra PNR-uppgifterna med skyddspolisens informationssystem, skulle man inte kunna förhindra eller avslöja terroristbrott i tillnärmelsevis lika hög grad. Utifrån ett nationellt effektivitetsperspektiv kan det anses vara av yttersta vikt att passagerarinformationen kan jämföras i den omfattning

det behövs även med skyddspolisens informationssystem. Till exempel en jämförelse med informationssystemet för polisärenden har inte en ens på långt när en lika effektiv terrorismhämmande inverkan, eftersom dess syfte när det gäller terroristbrott i princip är att utreda brott.

I skäl 23 i ingressen till direktivet hänvisas till rådets rambeslut 2006/960/RIF. Med stöd av detta rambeslut har det stiftats en nationell lag om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009). Enligt 3 § i lagen avses med information och underrättelser enligt 1) uppgifter i de personregister som avses i 2–4 och 6 § i lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Bestämmelser om skyddspolisens register ingår i 5 § i lagen om behandling av personuppgifter i polisens verksamhet, vilket innebär att lagen inte tillämpas i skyddspolisens verksamhet. Trots detta får skyddspolisens uppgifter inte ha ett sämre skydd än den övriga polisens uppgifter för vilkas del det i 7 § i lagen om informations- och underrättelseutbyte (26/2009) föreskrivs om vägran att lämna ut information och underrättelser, om utlämnandet av informationen kan kränka Finlands suveränitet eller äventyra Finlands säkerhet eller andra väsentliga nationella intressen. Grunden för vägran ska således i sak tillämpas också på skyddspolisens verksamhet, även om lagen i fråga formellt inte tillämpas på verksamheten.

I gällande lag om behandlingen av personuppgifter i polisens verksamhet utgår man från att uppgifterna i skyddspolisens funktionella datasystem i allmänhet är sådana att utlämnande av dem kan äventyra statens säkerhet (RP 39/1994 s. 21). Ett uttryck för detta är också att bestämmelserna om skyddspolisens uppgifter enligt 24 § 1 mom. 9 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999) innehåller en sekretesspresumtion. Med anledning av det som anges ovan är utgångspunkten också i detta lagförslag att det för utlämningen av uppgifter krävs samtycke av skyddspolisen. Med andra ord ska skyddspolisen bedöma om utlämningen av uppgifter kan äventyra statens säkerhet eller andra väsentliga nationella intressen.

Med avseende på uppgifternas sekretess är det stora skillnader mellan skyddspolisens och den övriga polisens informationssystem. Skillnaderna i sin tur uttrycker varför uppgifter som noterats vid en jämförelse med skyddspolisens informationssystem som regel inte kan lämnas vidare i motsats till exempelvis utlämningen av uppgifter från informationssystemet för polisärenden. Dessutom talar de begränsningar som gäller skyddspolisens utbyte av information för den föreslagna bestämmelsen. Jämfört med den övriga polisens informationssystem betonas i skyddspolisens system de s.k. reglerna om tredje land. Skyddspolisens verksamhet grundar sig i betydande grad på internationellt utbyte av information, och dess informationssystem innehåller i stor utsträckning personuppgifter som inhämtats i sådana sammanhang. Enligt 1 § 2 mom. i gällande lag om behandling av personuppgifter i polisens verksamhet ska utöver vad som föreskrivs i denna lag iakttas internationella avtal som är bindande för Finland. I de avtal som handlar om utbyte av information och som ger skyddspolisen nödvändig information för att den ska kunna sköta sina uppdrag finns det generellt en skyldighet att iaktta de begränsningar som gäller användningen av uppgifter. Det faktum att rätten till insyn enligt 45 § i lagen om behandling av personuppgifter i polisens verksamhet inte överhuvudtaget gäller skyddspolisens informationssystem talar för krav på ett särskilt samtycke i förhållande till övriga register. Någon liknande begränsning gäller inte exempelvis informationssystemet för polisärenden. Syftet med skyddspolisens och den övriga polisens register skiljer sig från varandra, vilket i hög grad påverkar möjligheterna att lämna ut uppgifter ur registret.

Vid enheten för passagerarinformation får enligt 6 mom. i paragrafen de passageraruppgifter som avses i denna paragraf behandlas bara av de tjänstemän som tillsatts för uppgiften.

7 §. *Utlämnande av passageraruppgifter till behöriga myndigheter.* Enligt paragrafen ska de passageraruppgifter om personer som har identifierats genom den behandling av passageraruppgifter som avses i 6 § 1 mom. 1 punkten eller resultaten av behandlingen av uppgifterna lämnas ut till de behöriga myndigheterna så att de kan utreda personernas delaktighet i terroristbrott eller grov brottslighet. Uppgifterna eller resultaten av behandlingen av uppgifterna får lämnas ut till de behöriga myndigheterna även på motiverad begäran som bygger på tillräckliga observationer. De uppgifter som avses i detta moment får lämnas ut bara fall för fall. Dataskyddsombudet vid enheten för passagerarinformation ska ha åtkomst till passageraruppgiftssamlingen.

Enligt artikel 6.6 i PNR-direktivet ska enheten för passagerarinformation i en medlemsstat översända PNR-uppgifterna beträffande personer som har identifierats i enlighet med punkt 2 a (bedömning av passagerare före ankomst eller avresa) eller resultaten av behandlingen av dessa uppgifter till de behöriga myndigheter som avses i artikel 7 i samma medlemsstat för vidare granskning. Sådana överföringar får bara göras i enskilda fall och, vid automatisk behandling av PNR-uppgifter, efter individuell icke-automatisk granskning. Enligt artikel 6.2 b i direktivet ska enheten för passagerarinformation i enskilda fall besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter eller resultaten av behandlingen av uppgifter. Enligt artikel 6.7 i direktivet ska medlemsstaterna se till att dataskyddsombudet har åtkomst till alla uppgifter som enheten för passagerarinformation behandlar. Genom den föreslagna 7 § genomförs artikel 6.2 b, 6.6 och 6.7 i PNR-direktivet.

8 §. *Utbyte av passageraruppgifter mellan medlemsstater.* Enligt 1 mom. i paragrafen får enheten för passagerarinformation begära passageraruppgifter av en enhet för passagerarinformation i en annan medlemsstat i syfte att förhindra terroristbrott eller andra grova brott. Begäran ska motiveras. Enheten för passagerarinformation ska till de behöriga myndigheterna lämna ut de passageraruppgifter eller de resultat av behandlingen av uppgifterna som den tagit emot av en enhet för passagerarinformation i en annan medlemsstat.

I artikel 9.2 i PNR-direktivet konstateras det att enheten för passagerarinformation i en medlemsstat ska ha rätt att vid behov begära att en enhet för passagerarinformation i en annan medlemsstat tillhandahåller PNR-uppgifter som lagrats i den senares databas på vissa närmare villkor, om den begärande enheten för passagerarinformation anser begäran vara nödvändig för att bekämpa terroristbrott eller grov brottslighet. Enligt artikel 9.1 i PNR-direktivet ska bland annat enheterna för passagerarinformation i de mottagande medlemsstaterna översända den mottagna informationen till sina behöriga myndigheter. Genom det föreslagna 1 mom. genomförs delvis artikel 9.1 och 2 i PNR-direktivet.

Enligt 2 mom. i paragrafen ska enheten för passagerarinformation lämna ut uppgifterna om personer som den identifierat genom sådan behandling av passageraruppgifter som avses i 6 § 1 mom. 1 punkten till motsvarande enheter för passagerarinformation i andra medlemsstater. De uppgifter som lämnas ut ska omfatta alla relevanta och nödvändiga passageraruppgifter om personer som identifierats genom behandlingen eller resultaten av behandlingen av uppgifterna. Enheten för passagerarinformation får dessutom lämna ut passageraruppgifter eller resultaten av behandlingen av uppgifterna till en enhet för passagerarinformation i en annan medlemsstat på dennes motiverade begäran.

När personer i samband med en bedömning av passagerare identifieras av en enhet för passagerarinformation ska medlemsstaten enligt artikel 9.1 i PNR-direktivet se till att enheten för passagerarinformation översänder alla relevanta och nödvändiga PNR-uppgifter eller resultaten av en eventuell behandling av dessa uppgifter till motsvarande enheter i de andra medlemsstaterna. I artikel 9.2 i PNR-direktivet konstateras det att enheten för passagerarinformat-

ion i en medlemsstat ska ha rätt att vid behov begära att en enhet för passagerarinformation i en annan medlemsstat tillhandahåller PNR-uppgifter som lagrats i den senares databas på vissa närmare villkor om den begärande enheten för passagerarinformation anser begäran vara nödvändig för att bekämpa terroristbrott eller grov brottslighet. Av artikel 9.1 framgår inte den ändamålsenliga principen att uppgifterna ska lämnas till enheten eller enheterna för passagerarinformation i den eller de medlemsstater som identifieringen hänsyftar till. Genom det föreslagna 2 mom. genomförs delvis artikel 9.1 och 2 i PNR-direktivet.

Enligt 3 mom. i paragrafen kan de behöriga myndigheterna direkt av en enhet för passagerarinformation i en annan medlemsstat begära passageraruppgifter när det behövs i nödfall eller för att bekämpa terrorism och grov brottslighet. Begäran ska motiveras och meddelande om den ska skickas till enheten för passagerarinformation i Finland. Under motsvarande förutsättningar får enheten för passagerarinformation i Finland lämna ut passageraruppgifter till de behöriga myndigheterna i en annan medlemsstat på deras begäran.

Enligt artikel 9.3 i PNR-direktivet får endast i nödfall och för att bekämpa terroristbrott och grov brottslighet en medlemsstats behöriga myndigheter vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om utlämnande av PNR-uppgifter som finns lagrade i den enhetens databas. Begäran från de behöriga myndigheterna ska motiveras. En kopia av begäran ska alltid skickas till enheten för passagerarinformation i den begärande medlemsstaten. I alla andra fall ska de behöriga myndigheterna översända sina framställningar via enheten för passagerarinformation i den egna medlemsstaten. Genom det föreslagna 3 mom. genomförs artikel 9.3 i PNR-direktivet.

9 §. *Överföring av passageraruppgifter till Europol.* Enheten för passagerarinformation får på motiverad begäran överföra PNR-uppgifter eller resultaten av behandlingen av uppgifterna till Europol för sådan behandling av uppgifterna som avses i kapitel IV i Europolförordningen i syfte att bekämpa terroristbrott och grov brottslighet när uppgifterna behöver överföras för att målen för medlemsstaternas behöriga myndigheters brottsbekämpningssamarbete och ömsesidiga samarbete i enlighet med artikel 3 i den förordningen ska nås.

Enligt artikel 10.1 i PNR-direktivet ska Europol inom ramen för sina befogenheter och för fullgörandet av sina arbetsuppgifter ha rätt att begära PNR-uppgifter eller resultaten av behandlingen av dessa uppgifter från enheterna för passagerarinformation i medlemsstaterna. Enligt artikel 10.2 får

Europol från fall till fall via Europols nationella enhet lämna in en elektronisk, vederbörligen motiverad begäran till enheten för passagerarinformation i en medlemsstat om översändande av specifika PNR-uppgifter eller resultaten av behandlingen av dessa uppgifter. Europol får lämna in en sådan begäran när detta är absolut nödvändigt för att stödja och stärka medlemsstaternas åtgärder för att förebygga, förhindra, upptäcka eller utreda ett specifikt terroristbrott eller grovt brott i den mån brottet i fråga omfattas av Europols behörighet enligt beslut 2009/371/RIF. I den motiverade begäran ska rimliga skäl anges till varför Europol anser att översändandet av PNR-uppgifterna eller resultaten av behandlingen av PNR-uppgifter väsentligt kommer att bidra till att brottet i fråga förebyggs, upptäcks eller utreds. Enligt artikel 10.3 ska Europol informera det dataskyddsombud som utsetts i enlighet med artikel 28 i beslut 2009/371/RIF om varje informationsutbyte enligt den här artikeln. Enligt artikel 10.4 ska informationsutbyte enligt denna artikel äga rum via Siena och i enlighet med beslut 2009/371/RIF. Det språk som används för framställningen och informationsutbytet ska vara det som gäller för Siena.

Europaparlamentets och rådets förordning (EU) 2016/794 (Europolförordningen) ersätter beslut 2009/371/RIF som nämns i PRN-direktivet. Bestämmelser som kompletterar Europolför-

ordningen har utfärdats i lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning (214/2017). Enligt 3 § 1 mom. i lagen tillåts de behöriga myndigheter i Finland som avses i artikel 2 a i Europolförordningen ha direktkontakt med Europol i enlighet med artikel 7.5 i den förordningen. Enligt artikel 7.5 ska i enlighet med punkt 2 den nationella enheten fungera som sambandsorgan mellan Europol och medlemsstaternas behöriga myndigheter. På villkor som fastställs av medlemsstaterna, inbegripet tidigare kontakt med den nationella enheten, får medlemsstaterna dock tillåta direktkontakt mellan sina behöriga myndigheter och Europol. Skyldigheten enligt PNR-direktivet att överföra uppgifter bara via en nationell enhet grundar sig på det upphävda beslutet. Eftersom förordningen tillåter också direktkontakt, är det inte ändamålsenligt att begränsa kontakterna till att ske bara via en nationell enhet. Genom den föreslagna 9 § genomförs artikel 10.1 och 2 i PNR-direktivet.

10 §. *Överföring av passageraruppgifter till tredjeländer*. I paragrafen föreskrivs om överföring av passageraruppgifter till tredjeländer. Enligt det föreslagna 1 mom. får enheten för passagerarinformation överföra passageraruppgifter och resultaten av behandlingen av uppgifterna till ett tredjeland bara i enskilda fall, om

1) de bestämmelser om allmänna principer för överföring av personuppgifter till tredjeländer som finns i 7 kap. 41 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) iakttas, och

2) uppgifterna behöver överföras för att sådana terroristbrott och sådan grov brottslighet som avses i denna lag ska kunna bekämpas.

Enligt artikel 11.1 a i PNR-direktivet får en medlemsstat överföra PNR-uppgifter och resultaten av behandling av sådana uppgifter som lagrats av enheten för passagerarinformation i enlighet med artikel 12 till ett tredjeland efter bedömning i det enskilda fallet, bara under förutsättning att de villkor som fastställs i artikel 13 i rambeslut 2008/977/RIF är uppfyllda. Rambeslut 2008/977/RIF har upphävts genom Europaparlamentets och rådets direktiv (EU) 2016/680 (dataskyddsdirektivet). I 7 kap. 41 § i regeringens proposition med förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, genom vilken dataskyddsdirektivet kommer att genomföras, behandlas allmänna principer för överföringen av personuppgifter till tredjeländer. Lagförslagets 7 kap. 41 § grundar sig på artikel 35, skäl 64 i ingressen och artikel 36.1 i dataskyddsdirektivet. Dessa ersätter de villkor som föreskrivs i artikel 13 i rambeslut 2008/977/RIF. Artikel 11.1 b i PNR-direktivet ställer som ytterligare villkor för överföring att överföringen är nödvändig för detta direktivs syften enligt artikel 1.2 (terroristbrott och grov brottslighet). Genom det föreslagna 1 mom. genomförs artikel 11.1 och 2 i PNR-direktivet.

I 2 mom. i paragrafen föreskrivs om villkoren för överföring, om passageraruppgifter eller resultat av behandlingen av uppgifterna vidareöverförs till ett annat tredjeland. Förutsättningen för överföringen är då, utöver det som nämns i 1 mom., att det är nödvändigt att överföra uppgifterna i syfte att bekämpa sådana terroristbrott och sådan grov brottslighet som avses i denna lag och att enheten för passagerarinformation har gett tillstånd till överföringen.

Enligt artikel 11.1 c i PNR-direktivet godtar det berörda tredjelandet att överföra uppgifterna till ett annat tredjeland bara om det är strikt nödvändigt för detta direktivs ändamål enligt artikel 1.2 och bara efter uttryckligt samtycke av medlemsstaten. Genom det föreslagna 2 mom. genomförs artikel 11.1 c i PNR-direktivet.

Enligt det föreslagna 3 mom. får med avvikelse från 1 mom. passageraruppgifter som överförts från en enhet för passagerarinformation i en annan medlemsstat överföras till ett tredjeland utan tillstånd av enheten för passagerarinformation i medlemsstaten i fråga bara om över-

föringen är av väsentlig betydelse för att man ska kunna reagera på ett i denna lag avsett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller ett tredjeland och tillstånd inte kan fås i tid. Enheten för passagerarinformation i medlemsstaten i fråga ska informeras om överföringen och överföringen ska registreras på behörigt sätt och kontrolleras i efterhand.

Enligt artikel 11.2 i PNR-direktivet ska överföring av PNR-uppgifter utan förhandssamtycke av den medlemsstat från vilken uppgifterna hämtades tillåtas i undantagsfall och bara om a) överföringen är absolut nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller ett tredjeland, och b) förhandssamtycke inte kan erhållas i tid. Den myndighet som ansvarar för att ge samtycke ska informeras utan dröjsmål och överföringen ska vederbörligen registreras samt genomgå efterhandskontroll. Genom det föreslagna 3 mom. genomförs artikel 11.2 i PNR-direktivet.

Innan passageraruppgifter överförs till de behöriga myndigheterna i ett tredjeland ska enligt 4 mom. i paragrafen enheten för passagerarinformation förvissa sig om att tredjelandets planerade användning av uppgifterna är förenlig med villkoren och skyddsåtgärderna enligt denna paragraf. Dataskyddsombudet vid enheten för passagerarinformation ska informeras om överföringen av uppgifterna.

Enligt artikel 11.3 i PNR-direktivet ska medlemsstaterna överföra PNR-uppgifter till behöriga myndigheter i tredjeländer på villkor som är förenliga med detta direktiv bara efter att ha förvissat sig om att mottagarnas planerade användning av uppgifterna är förenlig med dessa villkor och skyddsåtgärder. Enligt artikel 11.4 ska dataskyddsombudet vid enheten för passagerarinformation i den medlemsstat som har överfört PNR-uppgifterna informeras varje gång medlemsstaten överför PNR-uppgifter enligt denna artikel. Genom det föreslagna 4 mom. genomförs artikel 11.3 och 4 i PNR-direktivet.

11 §. *Utplåning och maskering av passageraruppgifter och utlämnande av maskerade uppgifter*. Enligt 1 mom. i paragrafen ska passageraruppgifter som har överförts av ett lufttrafikföretag utplånas ur registret vid enheten för passagerarinformation när fem år har förflutit sedan de överfördes till enheten. När sex månader har förflutit sedan uppgifterna överfördes till enheten ska följande passageraruppgifter avskiljas från uppgifterna genom maskering: 1) namn, inklusive namn på andra passagerare i PNR-uppgifterna samt antal passagerare som reser tillsammans, 2) adress och andra kontaktuppgifter, 3) alla former av betalningsinformation, inbegripet faktureringsadress, om denna innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som PNR-uppgifterna avser eller andra personer, 4) uppgifter om bonusprogram, 5) allmänna anmärkningar, och 6) eventuell förhandsinformation som har samlats in om passagerare (API-uppgifter).

Enligt artikel 12.1 i PNR-direktivet ska medlemsstaterna se till att PNR-uppgifter som lämnas av lufttrafikföretag till enheten för passagerarinformation lagras i en databas vid enheten under en period på fem år efter överföringen till enheten för passagerarinformation i den medlemsstat på vars territorium flygningen ankom eller avgick. Denna skyldighet gäller dock inte om specifika PNR-uppgifter har överförts till en behörig myndighet och används i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, varvid den behöriga myndighetens lagring av uppgifterna i stället ska regleras av nationell rätt. Enligt artikel 12.2 ska vid utgången av en period på sex månader efter överföringen av de PNR-uppgifter som avses i punkt 1 alla PNR-uppgifter avidentifieras genom maskering av följande uppgifter[punkt 1–6 ovan], som kan användas för att omedelbart identifiera de passagerare som PNR-uppgifterna avser. Enligt artikel 12.4 ska medlemsstaterna se till att PNR-uppgifterna slutgiltigt raderas vid utgången av den period som avses i punkt 1. Genom det föreslagna 1 mom. genomförs artikel 12.1 och 2 i PNR-direktivet.

Enligt 2 mom. i paragrafen ska enheten för passagerarinformation utplåna resultaten av den behandling som avses i 6 § 1 mom. 1 punkten (bedömning av passagerare i samband med avresa och ankomst) när de behöriga myndigheterna eller vid behov en enhet för passagerarinformation i en annan medlemsstat har informerats om en träff. Om resultatet efter en granskning visar sig vara felaktigt får den felaktiga uppgiften, för att felaktiga träffar ska kunna undvikas i framtiden, bevaras till dess att uppgifterna har utplånats med stöd 1 mom. De behöriga myndigheter eller den enhet för passagerarinformation i en annan medlemsstat som resultaten av behandlingen lämnats ut till ska informeras om felaktiga resultat.

Enligt artikel 12.5 i PNR-direktivet ska resultaten av den behandling som avses i artikel 6.2 a bevaras bara av enheten för passagerarinformation så länge som krävs för att informera de behöriga myndigheterna och, i enlighet med artikel 9.1, för att informera enheterna för passagerarinformation i andra medlemsstater om en träff. Även om automatisk behandling som utförs efter en sådan individuell icke-automatisk granskning som avses i artikel 6.5 inte ger någon träff, får resultatet bevaras för att undvika framtida ”falska” träffar, så länge de bakomliggande uppgifterna inte har raderats enligt punkt 4 i den här artikeln. Genom det föreslagna 2 mom. genomförs artikel 12.5 i PNR-direktivet.

I 3 mom. i paragrafen föreskrivs om skyldigheten att utplåna passageraruppgifter omedelbart efter att de har mottagits, om de uppgifter som ett lufttrafikföretag har överfört till enheten för passagerarinformation innehåller andra än i 4 § 2 mom. nämnda passageraruppgifter.

Om PNR-uppgifter som överförs av lufttrafikföretag omfattar andra uppgifter än dem som anges i bilaga I, ska enligt artikel 6.1 andra meningen i PNR-direktivet enheten för passagerarinformation omedelbart och slutgiltigt radera dessa vid mottagandet. Genom det föreslagna 3 mom. genomförs artikel 6.1 andra meningen i PNR-direktivet.

Passageraruppgifter från vilka de uppgifter som avses i 1 mom. har avskilts genom maskering får enligt 4 mom. i paragrafen lämnas ut bara genom ett beslut av chefen för enheten för passagerarinformation eller av en av denne förordnad person som hör till personalen vid enheten för passagerarinformation. Om det är fråga om en begäran från en enhet för passagerarinformation i en annan medlemsstat krävs det dessutom att utlämnandet av uppgifterna rimligen kan antas vara behövligt för att terroristbrott och grov brottslighet ska kunna bekämpas.

Enligt artikel 12.3 i PNR-direktivet ska vid utgången av perioden på sex månader (tidsfrist för maskering av uppgifter) utlämnande av de fullständiga PNR-uppgifterna tillåtas bara a) om det rimligen kan antas vara nödvändigt för de ändamål som avses i artikel 6.2 b (begäran av en behörig myndighet), och b) efter tillstånd från i) en rättslig myndighet, eller ii) en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda, under förutsättning att dataskyddsombudet vid enheten för passagerarinformation informeras och att denne genomför en efterhandsutvärdering. Utlämningen av uppgifter efter maskering kan inte ses som en sådan åtgärd som ingår i polisens sedvanliga verksamhet, och att det därför inte skulle vara nödvändigt att särskilt föreskriva om den som vidtar åtgärden. För att utföra sina uppdrag enligt polislagen på de sätt som anges i olika lagar har polisen rätt att få och lämna ut personuppgifter. Utlämningen av personuppgifter för de syften som avses i PNR-direktivet hör till de åtgärder som påverkar individens rättigheter och skyldigheter, och det är därför motiverat att särskilt föreskriva också om den. Oberoende av att en sammanslutnings medlemmar, revisorer, verkställande direktör, styrelsemedlemmar eller arbetstagare är bundna av företags-, bank- eller försäkringshemlighet har polisen enligt 4 kap. 3 § 1 punkten i polislagen (872/2011) på begäran av en polisman som hör till befälet rätt att få information som behövs för att förhindra eller utreda brott. Med beaktande av att en polisman som hör till befälet enligt gällande lag har en omfattande rätt att få tillgång till konfidentiella

uppgifter, är det lämpligt att fastställa samma tröskel också för utlämningen av passagerar-uppgifter.

Om de uppgifter som enheten för passagerarinformation i en annan medlemsstat begärt har avidentifierats genom maskering, ska enligt artikel 9.2 i PNR-direktivet enheten för passagerarinformation bara tillhandahålla fullständiga PNR-uppgifter, om det rimligen kan antas vara nödvändigt för att bekämpa terroristbrott och grov brottslighet. Genom det föreslagna 4 mom. genomförs artikel 9.2 delvis samt artikel 12.3.

12 §. *Inskränkningar i rätten till insyn.* Med avvikelse från 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) gäller enligt 1 mom. i paragrafen rätten till insyn inte uppgifter om resultaten av behandlingen av passageraruppgifter. Enligt 2 mom. kan dataskyddsmyndigheten på begäran av en registrerad kontrollera att de uppgifter som avses i 1 mom. är lagenliga.

13 §. *Personuppgiftsansvarig för PNR-uppgifter.* Polisstyrelsen är personuppgiftsansvarig för det register som innehåller passageraruppgifter. Bestämmelsen är informativ till sin karaktär.

14 §. *Påföljdsavgift för lufttrafikföretag.* I paragrafen föreskrivs om påföljdsavgift för lufttrafikföretag. Enligt 1 mom. ska lufttrafikföretag som bryter mot skyldigheten i 4 § att överföra passageraruppgifter påföras en påföljdsavgift (påföljdsavgift för lufttrafikföretag). Avgiften är 3 000 euro för varje sådan flygning för vilken passageraruppgifter inte har överförts eller för vilken uppenbart bristfälliga uppgifter överförts.

Enligt artikel 14 i PNR-direktivet ska medlemsstaterna särskilt fastställa bestämmelser om sanktioner, inklusive ekonomiska sanktioner, mot lufttrafikföretag som inte översänder uppgifter i enlighet med direktivet eller som inte översänder uppgifterna i det fastställda formatet. Sanktionerna ska vara effektiva, proportionella och avskräckande. Om man ser till principerna och påföljdens omfattning överensstämmer bestämmelsen med 20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) om lufttrafikföretags skyldighet att lämna på förhand fastställda passageraravgifter till gränskontrollmyndigheten. Påföljderna av brott mot skyldigheten definieras i 179 § 1 mom. i utlänningslagen (301/2004). Genom bestämmelsen i fråga genomförs skyldigheten i artikel 4 i rådets direktiv 2004/82/EG, det s.k. API-direktivet, om lufttrafikföretags skyldighet att lämna förhandsinformation om passagerare och påföra de företag som inte översänder uppgifter eller översänder bristfälliga eller felaktiga uppgifter sanktioner som är effektiva, proportionella och avskräckande. Eftersom de uppgifter som avses i PNR-direktivet till viss del grundar sig på uppgifter från passagerarna själva, och lufttrafikföretagen inte har vare sig skyldighet eller möjlighet att kontrollera riktigheten, går det inte att ställa samma villkor för uppgifternas riktighet som när uppgifter översänds enligt API-direktivet. Därför bör det vara uppenbart att de uppgifter som har översänts är bristfälliga, innan en påföljdsavgift kan övervägas. Genom det föreslagna 1 mom. genomförs artikel 14 i PNR-direktivet.

Enligt 2 mom. i paragrafen påförs ingen påföljdsavgift för lufttrafikföretag om det vid överföringen av passageraruppgifterna har inträffat ett fel till följd av ouppmärksamhet som med beaktande av samtliga omständigheter är ursäktlig eller om det i övrigt med hänsyn till omständigheterna skulle vara oskäligt att påföra en avgift.

Enligt 3 mom. i paragrafen får påföljdsavgift för lufttrafikföretag inte påföras den som är misstänkt för samma gärning i en förundersökning eller åtalsprövning eller i ett brottmål som är anhängigt vid en domstol. Påföljdsavgift för lufttrafikföretag får inte heller påföras den som genom en lagakraftvunnen dom har dömts till straff för samma gärning eller som för brott mot

20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) har påförts påföljdsavgift för transportör enligt 179 § i utlänningslagen (301/2004).

15 §. *Hörande av lufttrafikföretag.* I paragrafen föreskrivs om rätten för lufttrafikföretag att bli hörda innan en påföljdsavgift för transportör påförs. Lufttrafikföretaget ska skriftligen ges tillfälle att avge en förklaring inom en tid som inte får vara kortare än två veckor.

16 §. *Påförande av påföljdsavgift för lufttrafikföretag.* Enligt den föreslagna paragrafen ska påföljdsavgift för lufttrafikföretag påföras av en polisman som hör till befälet vid enheten för passagerarinformation. Påföljdsavgiften ska betalas till staten. Avgiften anges i beslutet. Ett beslut om påförande av påföljdsavgift ska iakttas även om ändring har sökts, om inte besvärsmyndigheten bestämmer något annat. Eftersom Polisstyrelsen är personuppgiftsansvarig för registret över passageraruppgifter, kan polisen anses vara lämplig att påföra påföljdsavgifter.

17 §. *Betalningstid.* Enligt den föreslagna paragrafen ska påföljdsavgiften för lufttrafikföretag betalas inom en månad från det att lufttrafikföretaget har fått ta del av beslutet. På en påföljdsavgift som förfallit till betalning och som inte har betalats senast på förfallodagen tas det ut en dröjsmålsränta enligt den räntesats som avses i 4 § 1 mom. i räntelagen (633/1982).

18 §. *Verkställighet och ändringssökande.* I paragrafen föreskrivs det om hur påföljdsavgiften verkställs och om sökande av ändring. Enligt det föreslagna 1 mom. verkställer rättsregistercentralen påföljdsavgiften för lufttrafikföretag. Rättsregistercentralen ska underrättas om ett beslut av en myndighet eller domstol genom vilket påföljdsavgiften har sänkts eller avlyfts. Rättsregistercentralen ska utan ansökan betala tillbaka en påföljdsavgift som betalats utan grund. Enligt 2 mom. ska en påföljdsavgift som påförts med stöd av denna lag verkställas i den ordning som föreskrivs i lagen om verkställighet av böter. Enligt 3 mom. får ett beslut om påföljdsavgift för lufttrafikföretag överklagas genom besvär hos förvaltningsdomstolen på det sätt som föreskrivs i förvaltningsprocesslagen (586/1996). Förvaltningsdomstolens beslut får överklagas genom besvär bara om högsta förvaltningsdomstolen beviljar besvärstillstånd.

19 §. *Ikraftträdande.* Lagen föreslås träda i kraft samtidigt som lagförslag 1 den 2018. Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder kraft.

1.3 Lag om Enheten för grå ekonomi

12 §. *Behandling av personuppgifter och rätt till insyn.* Hänvisningen i paragrafens 2 mom. till 45 § i gällande lag om behandling av personuppgifter i polisens verksamhet ska ersättas med en hänvisning till 6 kap. 2 § i lagförslag 1 som innehåller bestämmelser om inskränkningar i den registrerades rätt till insyn.

1.4 Lag om kontrollavgift i kollektivtrafik

6 §. *Biljettkontrollörer.* I 5 mom. i paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 stället för lagen om behandling av personuppgifter i polisens verksamhet.

1.5 Lag om besöksförbud

15 §. *Registrering av besöksförbud.* I paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 i stället för gällande lag om behandling av personuppgifter i polisens verksamhet. Till paragrafen fogas samtidigt preciserande hänvisningar till de para-

grafer i lagförslag 1 som innehåller bestämmelser om registrering och utplåning av uppgifter om besöksförbud.

1.6 Lag om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

17 §. *Teknisk övervakning.* I 5 mom. i paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 stället för lagen om behandling av personuppgifter i polisens verksamhet.

1.7 Lag om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor

9 §. ***Registrering av skyddsåtgärder.*** I paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 stället för lagen om behandling av personuppgifter i polisens verksamhet. Till paragrafen fogas samtidigt en preciserande hänvisning till paragrafen som innehåller bestämmelser om behandling av uppgifter som gäller skyddsåtgärder.

1.8 Lag om brottsbekämpning inom Tullen

2 kap. **Tullens befogenheter vid tullbrottsbekämpning**

15 §. *Identifiering.* I hänvisningen i 2 mom. i paragrafen till de personregister som avses i 2 § i gällande lag om behandling av personuppgifter i polisens verksamhet föreslås en ändring så att den i stället avser 2 kap. 3 och 5 § i lagförslag 1. Hänvisningen överensstämmer i sak med den nuvarande med undantag för de observationsuppgifter som ingår i de personregister som avses i 2 § i gällande lag.

1.9 Lag om privata säkerhetstjänster

86 §. *Uppgifter för tillsynen över säkerhetsbranschen.* Enligt sista meningen i gällande 86 § finns närmare bestämmelser om uppgifter för tillsynen över säkerhetsbranschen i lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Det föreslås att förhållandet mellan lagen om behandling av personuppgifter i polisens verksamhet och lagen om privata säkerhetstjänster tydliggörs genom en ändring av den sista meningen så att lagförslag 1 tillämpas på behandlingen av uppgifter för tillsynen över säkerhetsbranschen.

1.10 Lag om militär disciplin och brottsbekämpning inom försvarsmakten

42 §. *Rätt att få uppgifter ur vissa myndigheters register.* I 2 mom. i paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 stället för lagen om behandling av personuppgifter i polisens verksamhet.

1.11 Lag om behandling av personuppgifter inom Tullen

17 §. *Utlämnande av uppgifter till andra myndigheter.* I 3 mom. i paragrafen föreslås en ändring som innebär att hänvisningen avser bestämmelserna i lagförslag 1. Momentet överensstämmer i sak med gällande lag.

1.12 Tvångsmedelslag

9 kap. **Tvångsmedel i samband med särskilda undersökningsmetoder**

4 §. *Bestämning och registrering av dna-profiler.* I 3 mom. i paragrafen föreslås en lagteknisk ändring som innebär att hänvisningen avser lagförslag 1 stället för lagen om behandling av personuppgifter i polisens verksamhet.

10 kap. **Hemliga tvångsmedel**

62 §. *Begränsning av partsoffentlighet i vissa fall.* Det föreslås att paragrafens 1 mom. ändras så att det i stället för till personuppgiftslagen och polisens gällande personuppgiftslag hänvisas till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten som ska tillämpas på den registrerades rätt till insyn.

1.13 Skjutvapenlagen

113 §. *Polisens skyldighet att föra register.* I paragrafens 2 mom. föreslås en lagteknisk ändring som innebär att hänvisningen till den gällande lagen om behandling av personuppgifter i polisens verksamhet ersätts med en hänvisning till lagförslag 1.

1.14 Lotterilagen

42 b §. *Tillsynsregister över lotterier.* Enligt gällande lydelse i 2 mom. finns bestämmelser om register som förs av polisen i lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Förhållandet mellan polisväsendets personuppgiftslag och lotterilagen ska förtydligas genom att den sista meningen ändras så att lagförslag 1 tillämpas på behandlingen av personuppgifter i polisens register.

1.15 Lagen om nödcentralsverksamhet

17 §. *Information som ska lagras i nödcentralsdatasystemet.* Paragrafens 4 mom. ändras så att där hänvisas till 4 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till 6 kap. i lagen om behandling av personuppgifter i polisens verksamhet, vilka innehåller bestämmelser om den registrerades rättigheter.

19 §. *Rätt att få information ur registren.* Hänvisningarna i 1 mom. 1 och 11 punkten i paragrafen till de informationssystem som avses i polisens gällande personuppgiftslag ersätts med en hänvisning till bestämmelser i lagförslag 1. Hänvisningen motsvarar i sak den gällande lagen.

1.16 Lag om utlänningsregistret

3 a §. *Användning av fingeravtrycksuppgifter i delregistret för främlingspass och resedokument för flykting.* Det föreslås att paragrafens 2 mom. ändras så att det i momentet hänvisas till bestämmelser i lagförslag 1. Hänvisningen motsvarar i sak den gällande lagen.

3 b §. *Användning och jämförelse av fingeravtrycksuppgifter i delregistret för ansökningsärenden.* Hänvisningen i 2 mom. till det informationssystem för förvaltningsärenden som avses i 3 § i lagen om behandling av personuppgifter i polisens verksamhet ersätts med en allmännare hänvisning till polisens register, eftersom fingeravtryck som med stöd av 131 § i utlänningslagen registreras i polisens register inte ska vara en del av informationssystemet för förvaltningsärenden. Dessutom ska paragrafhänvisningarna i 2 och 3 mom. ändras så att det i dem hänvisas till bestämmelser i lagförslag 1.

4 a §. *Den registrerades rättigheter.* Det föreslås att paragrafens 1 mom. ändras så att det i stället för till personuppgiftslagen och polisens gällande personuppgiftslag hänvisas till lagen

om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten där det finns bestämmelser om den registrerades rätt till insyn.

1.17 Utlänningslagen

131 §. *Upptagande av signalement.* Hänvisningen till 9 § i lagen om utlänningsregistret i paragrafens 2 mom. ersätts med en hänvisning till 5 kap. 2 § i lagförslag 1, i vilken det föreskrivs om utplåning av signalement som i enlighet med 131 § registrerats i polisens register. Även i 23 § i polisens gällande personuppgiftslag finns det bestämmelser om utplåning av signalement, men i 131 § 2 mom. i utlänningslagen hänvisas det felaktigt till en bestämmelse om utplåning i 9 § i lagen om utlänningsregistret. Dessutom föreslås det att 3 mom. ändras så att där hänvisas till bestämmelser i lagförslag 1. I sak motsvarar 3 mom. den gällande lagen.

1.18 Lagen om penninginsamlingar

27 §. *Tillsynsregister över penninginsamlingar.* Enligt gällande lydelse i 2 mom. finns bestämmelser om tillsynsregistret över penninginsamlingar i lagen om behandling av personuppgifter i polisens verksamhet (761/2003). Förhållandet mellan polisväsendets personuppgiftslag och lagen om penninginsamlingar ska förtydligas genom att den sista meningen ändras så att lagförslag 1 tillämpas på behandlingen av personuppgifter i polisens register.

1.19 Passlagen

29 §. *Passregister.* Enligt gällande lydelse i paragrafens 1 mom. ska polisen föra ett register där det förs in sådana uppgifter om en persons identitet som avses i 3 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet (761/2003) och sådana passuppgifter, bilduppgifter och fingeravtrycksuppgifter i pass som avses i 3 § 3 mom. 2–4 punkten i nämnda lag. Eftersom det i lagförslag 1 inte finns detaljerade bestämmelser om passregistrets innehåll, föreslås det att den reglering som gäller registrets innehåll ska överföras till 29 § 1 mom. i passlagen. Innehållet motsvarar i sak det innehåll som anges i 3 § i polisens gällande personuppgiftslag. Dessutom ska hänvisningarna till polisens gällande personuppgiftslag i paragrafens 2 mom. ändras till hänvisningar till de bestämmelser i lagförslag 1, i vilka det föreskrivs om användning, utlämnande och utplåning av uppgifter i passregistret samt om skyddet av känsliga personuppgifter.

1.20 Lagen om identitetskort

17 §. *Förvägrande av identitetskort och identitetskort utan rätt att resa.* Hänvisningen i 5 mom. till det informationssystem för förvaltningsärenden som avses i 3 § i lagen om behandling av personuppgifter i polisens verksamhet ersätts med en allmännare hänvisning till polisens register, eftersom det i lagförslag 1 till skillnad från i den gällande lagen inte ska föreskrivas om informationssystem för förvaltningsärenden.

31 §. *Identitetskortsregister.* Enligt gällande lydelse i paragrafens 1 mom. ska polisen föra ett register där det förs in sådana uppgifter om en persons identitet som avses i 3 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet och sådana uppgifter om identitetskort och bilduppgifter som avses i 3 § 3 mom. 2 och 3 punkten i den lagen. Eftersom det i lagförslaget inte finns detaljerade bestämmelser om identitetskortsregistrets innehåll, föreslås det att den reglering som gäller registrets innehåll ska överföras till 31 § 1 mom. i lagen om identitetskort. Innehållet motsvarar i sak det innehåll som anges i 3 § i polisens gällande personuppgiftslag. Dessutom ska hänvisningarna till polisens gällande personuppgiftslag i paragrafens 2 mom. ändras till hänvisningar till de bestämmelser i lagförslaget, i vilka det föreskrivs om användning, utlämnande och utplåning av uppgifter i identitetskortsregistret.

1.21 Lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet

3 §. *Definition av information och underrättelser.* Hänvisningarna till bestämmelser i polisens gällande personuppgiftslag ändras till hänvisningar till bestämmelser i lagförslag 1. Hänvisningarna motsvarar i sak den gällande lagen.

5 §. *Utlämnande av information och underrättelser på begäran.* Hänvisningarna i 2 och 3 mom. till bestämmelser i polisens gällande personuppgiftslag ändras till hänvisningar till de bestämmelser i lagförslag 1, i vilka det föreskrivs om förutsättningarna för utlämnande av information och beslutsfattande som gäller utlämnande av information.

6 §. *Utlämnande av information och underrättelser på eget initiativ.* Hänvisningarna i 2 och 3 mom. till bestämmelser i polisens gällande personuppgiftslag ändras till hänvisningar till de bestämmelser i lagförslag 1, i vilka det föreskrivs om förutsättningarna för utlämnande av information och beslutsfattande som gäller utlämnande av information.

1.22 Lagen om genomförande av vissa bestämmelser i beslutet om Eurojust

10 §. *Utlämnande av personuppgifter till Eurojust.* Hänvisningen i 2 mom. till 29 § i polisens gällande personuppgiftslag ersätts med en hänvisning till 4 kap. 5 § i lagförslag 1 som ska tilllämpas på utlämnande av uppgifter ur polisens personregister till Eurojust.

1.23 Lagen om verkställighet av böter

1 §. *Lagens tillämpningsområde.* Till 1 mom. fogas en ny 12 punkt i vilken konstateras att i den ordning som föreskrivs i lagen om verkställighet av böter verkställs också den påföljdsavgift för lufttrafikföretag som avses i 14 § i lagförslag 2.

19 §. *Efterlysning.* Hänvisningen i 2 mom. till de uppgifter som nämns i 2 § 5 punkten i den upphävda förordningen om polisens personregister (1116/1995) ersätts med en beskrivning av de uppgifter som ska anges i efterlysningen.

1.24 Lagen om stark autentisering och betrodda elektroniska tjänster

7 b §. *Information om giltighet för pass eller identitetskort.* Hänvisningen till polisens informationssystem för förvaltningsärenden ersätts med en allmännare hänvisning till polisens informationssystem, eftersom det i lagförslag 1 till skillnad från i den gällande lagen inte ska föreskrivas om informationssystem för förvaltningsärenden.

1.25 Polislagen

5 kap. **Hemliga metoder för inhämtande av informati**on

41 §. *Behandling av uppgifter om en informationskälla och betalning av arvode.* I paragrafens 1 mom. föreslås en lagteknisk ändring som innebär att hänvisningen till polisens gällande personuppgiftslag ersätts med en hänvisning till lagförslag 1.

60 §. *Begränsning av partsoffentlighet i vissa fall.* Det föreslås att paragrafens 1 mom. ändras så att det i stället för till personuppgiftslagen och polisens gällande personuppgiftslag hänvisas

till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten där det finns bestämmelser om den registrerades rätt till insyn.

1.26 Lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning

5 §. *Nationell tillsynsmyndighet.* Hänvisningen till dataombudsmannen ersätts med en hänvisning till dataskyddsmyndigheten, som ska vara den nationella tillsynsmyndighet som avses i Europolförordningen.

1.27 Lagen om behandlingen av personer i förvar hos polisen

1 kap. **Allmänna bestämmelser**

7 §. *Ställningen för en väktare som är anställd av en innehavare av näringstillstånd inom säkerhetsbranschen.* Hänvisningen i 5 mom. till de informationssystem som avses i 2 kap. i polisens gällande personuppgiftslag ersätts med en hänvisning till polisens personregister, på vilka lagförslag 1 ska tillämpas. Hänvisningen motsvarar i sak den gällande lagen.

2 kap. **Intagning i förvaringslokal**

4 §. *Ankomstgranskning och registrering av uppgifter.* I paragrafens 2 mom. föreslås en lagteknisk ändring som innebär att hänvisningen till polisens gällande personuppgiftslag ersätts med en hänvisning till lagförslag 1.

7 kap. **Besök och andra kontakter utanför förvaringslokalen**

1 §. *Besök.* Hänvisningen i 2 mom. till vad som bestäms i polisens gällande personuppgiftslag ersätts med en hänvisning till de bestämmelser i lagförslag 1 som ska tillämpas på förvaring och utplåning av upptagningar som uppkommit vid övervakning.

5 §. *Besöksförbud.* Enligt gällande lydelse i 5 mom. finns bestämmelser om registrering av uppgifter i informationssystemet för polisärenden i lagen om behandling av personuppgifter i polisens verksamhet. Förhållandet mellan polisväsendets personuppgiftslag och lagen om behandlingen av personer i förvar hos polisen ska förtydligas genom att 5 mom. ändras så att lagförslag 1 tillämpas på behandlingen av uppgifter om besöksförbud i polisens personregister.

12 kap. **Teknisk övervakning**

2 §. *Upptagning.* Hänvisningen i 3 mom. till vad som bestäms i polisens gällande personuppgiftslag ersätts med en hänvisning till de bestämmelser i lagförslag 1 som ska tillämpas på förvaring och utplåning av upptagningar som uppkommit vid teknisk övervakning.

1.28 Lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet

5 §. *PTG-kriminalunderrättelseenheter.* Den riksomfattande kriminalunderrättelseenhet som i 5 § i lagförslag 2 föreslås bli fastställd som nationell enhet för passagerarinformation blir i 1 mom. i paragrafen fastställd som permanent. Utöver den nationella enheten kan det inrättas regionala och lokala PTG-kriminalunderrättelseenheter. I den sista meningen i 1 mom. stryks samtidigt hänvisningen till de särskilda polisbefogenheter som avses i 8 § i den upphävda polislagen (493/1995), eftersom det inte föreskrivs om dem i den gällande polislagen.

6 §. *Behandlingen av uppgifter vid PTG-kriminalunderrättelseenheterna.* I 1 mom. föreslås en ändring som innebär att i fråga om behandlingen av personuppgifter vid en PTG-kriminalunderrättelseenhet gäller vad som föreskrivs i lagen om behandling av personuppgifter i polisens verksamhet (/), lagen om behandling av personuppgifter vid gränsbevakningsväsendet (/) och lagen om behandling av personuppgifter inom Tullen (/). PTG-myndigheterna får också i fortsättningen inrätta tillfälliga register för brottsanalys i enlighet med bestämmelserna i lagarna om behandling av personuppgifter i polisens verksamhet, vid gränsbevakningsväsendet och inom Tullen. Också den personuppgiftsansvarige bestäms enligt de här lagarna så att den PTG-myndighet som har inrättat registret fortsättningsvis är personuppgiftsansvarig.

1.29 Säkerhetsutredningslagen

25 §. *Informationskällor vid normal säkerhetsutredning av person.* Hänvisningen i 1 mom. 4 punkten till informationssystemet för polisärenden, informationssystemet för förvaltningsärenden och skyddspolisens funktionella informationssystem, vilka avses i polisens gällande personuppgiftslag, ersätts med en hänvisning till bestämmelser i lagförslag 1. Hänvisningen motsvarar i sak den gällande lagen.

32 §. *Begränsning av användningen av uppgifter i säkerhetsutredning av person.* Hänvisningen i 1 mom. 2 punkten till iakttagelser i informationssystemet för polisärenden och hänvisningen i 3 mom. till informationssystemet för polisärenden, informationssystemet för förvaltningsärenden och skyddspolisens funktionella informationssystem ersätts med en hänvisning till bestämmelser i lagförslag 1. Begränsningarna av användningen hindrar dock inte centralkriminalpolisen från att göra en sådan anmälan som avses i 25 § 2 mom. utifrån uppgifter som avses i 2 kap. 4 § 2 mom. i lagförslag 1.

49 §. *Avförande av uppgifter ur registret över säkerhetsutredningar.* Hänvisningen till personuppgiftslagen i paragrafens sista mening ersätts med en hänvisning till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten som ska tillämpas på avförande av uppgifter ur registret över säkerhetsutredningar.

56 §. *Dataskyddsmyndighetens rätt att utöva tillsyn.* Hänvisningarna till dataombudsmannen i paragrafens rubrik och i 1 och 2 mom. ändras till en hänvisning till dataskyddsmyndigheten. Dessutom ersätts hänvisningen till personuppgiftslagen i 2 mom. med en hänvisning till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten där det finns bestämmelser om dataskyddsmyndighetens rätt att utöva tillsyn över och få information om behandlingen av personuppgifter.

61 §. *Hänvisning till straffbestämmelser.* Hänvisningen till personregisterbrott ändras på motsvarande sätt som en föreslagen ändring i strafflagen till en hänvisning till dataskyddsbrott. Samtidigt stryks hänvisningen till den personregisterförseelse som avses i 48 § 2 mom. i personuppgiftslagen.

1.30 Lagen om centralen för utredning av penningtvätt

3 §. *Registret för förhindrande, avslöjande och utredning av penningtvätt och av finansiering av terrorism.* Hänvisningen till dataombudsmannen i 6 och 8 mom. ersätts med en hänvisning till dataskyddsmyndigheten. I paragrafens 9 mom. föreslås en lagteknisk ändring som innebär att hänvisningen till polisens gällande personuppgiftslag ersätts med en hänvisning till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till lagförslag 1.

4 §. *Centralens rätt att få, använda och lämna ut uppgifter.* I 4 mom. görs en teknisk justering genom en hänvisning till en behörig tillsynsmyndighet som avses i lagen om förhindrande av penningtvätt och av finansiering av terrorism.

1.31 Lagen om förhindrande av penningtvätt och av finansiering av terrorism

4 kap. **Rapporteringsskyldighet, tystnadsplikt och avbrytande av transaktioner**

3 §. *Bevarande av uppgifter om tvivelaktiga affärstransaktioner.* Hänvisningen till dataombudsmannen i 2 mom. ersätts med en hänvisning till dataskyddsmyndigheten.

4 §. *Tystnadsplikt och undantag från tystnadsplikten i fråga om tvivelaktiga affärstransaktioner.* Hänvisningen till personuppgiftslagen i 4 mom. ersätts med en hänvisning till dataskyddsförordningen där det föreskrivs om de skyldigheter i fråga om skydd för personuppgifter som avses i momentet.

7 kap. **Tillsyn**

8 §. *Förfarande vid rapportering av misstänkta överträdelser hos en rapporteringsskyldig.* Hänvisningen till dataombudsmannen i 3 mom. ersätts med en hänvisning till dataskyddsmyndigheten.

9 §. *System för mottagande av rapport om misstanke om överträdelser.* Hänvisningen till dataombudsmannen i 3 mom. ersätts med en hänvisning till dataskyddsmyndigheten.

1.32 Lagen om Polisyrkeshögskolan

49 §. *Hantering av känslig information.* Hänvisningen i 1 mom. till sådana känsliga personuppgifter som avses i 11 § 3 och 4 punkten i personuppgiftslagen ersätts med en uppräkning i 1 mom. av de uppgifter som anges i nämnda 3 och 4 punkten. Detta motsvarar i sak den gällande lagen.

1.33 Lagen om vittnesskyddsprogram

13 §. *Register över vittnesskyddsprogram.* Hänvisningarna till personuppgiftslagen i 1 och 3 mom. ersätts med en hänvisning till lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till dess tillämpningsområde hör den behandling av personuppgifter som centralkriminalpolisen genomför då de sköter uppgifter som det föreskrivs om i lagen om vittnesskyddsprogram.

2 Närmare bestämmelser och föreskrifter

[*Kompletteras vid behov under den fortsatta beredningen.*]

3 Ikraftträdande

Lagen föreslås träda i kraft den 2018 eller så snart som möjligt. Dataskyddsförordningen tillämpas från och med den 25 maj 2018. Medlemsstaterna ska senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa dataskyddsdirektivet. Medlemsstaterna ska tillämpa dessa bestämmelser från och med den 6 maj 2018. Medlemsstaterna ska senast den 25 maj 2018 sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa PNR-direktivet.

4 Förhållande till grundlagen samt lagstiftningsordning

4.1 Skyddet för privatlivet

Behandlingen av personuppgifter

Bestämmelserna i lagförslagen är betydelsefulla med tanke på grundlagens 10 § som gäller skyddet för privatlivet. Utgångspunkten för skyddet för privatlivet i 10 § i grundlagen är att var och en har rätt att leva sitt eget liv utan myndigheternas eller andra utomståendes godtyckliga eller omotiverade inblandning i hans eller hennes privatliv. Enligt 10 § 1 mom. i grundlagen utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Grundlagsutskottets vedertagna praxis har varit att lagstiftarens handlingsutrymme begränsas både av den här bestämmelsen och av att skyddet för personuppgifter delvis ingår i samma moment som skyddet för privatlivet. På det hela taget handlar det om att lagstiftaren måste tillgodose denna rätt på ett sätt som är godtagbart med avseende på de grundläggande fri- och rättigheterna överlag. För skyddet för personuppgifter har utskottet ansett det viktigt att det i lag åtminstone ingår bestämmelser om syftet med registreringen, innehållet i de berörda personuppgifterna, tillåtna användningsändamål inklusive rätt att lämna ut uppgifterna, uppgifternas förvaringstid i personregistret och de registrerades rättssäkerhet. Dessutom ska regleringen av dessa faktorer på lagnivå vara heltäckande och detaljerad. Dessa synpunkter ska tillämpas även på en bredare reglering av användningen av personuppgifter (se till exempel GrUU 29/2016 rd, GrUU 13/2016 rd, s. 3–4, på finska, GrUU 14/2009 rd, s. 2, GrUU 11/2008 rd, s. 3/I, på finska, och GrUU 51/2002 rd, s. 1–2).

I Europeiska unionens stadga om de grundläggande rättigheterna tryggas respekten för privatlivet i artikel 7 och skyddet för personuppgifter i artikel 8. EU-domstolens domar på dessa punkter är utslagsgivande för det viktigaste innehållet i respekten för privatlivet och skyddet för personuppgifter. På samma sätt har artikel 8 i Europakonventionen, som gäller skydd för privatlivet, i Europadomstolens rättspraxis ansetts innefatta skyddet för personuppgifter. Europadomstolen har vid flera tillfällen konstaterat att enbart det att personuppgifter lagras i myndigheters register innebär en inskränkning av integritetsskyddet (se till exempel S. och Marper mot Förenade kungariket, 4.12.2008, punkt 67 i domen, Leander mot Sverige, 26.3.1987, punkt 48 i domen). Det som personuppgifterna senare används för är till denna del inte av betydelse (Amann mot Schweiz, 16.2.2000, punkt 69 i domen). För att bedöma om de uppgifter som myndigheterna har samlat in hänför sig till privatlivets delområden har domstolen i synnerhet beaktat den kontext som personuppgifterna samlats in och behandlats i samt de konsekvenser som kontexten kan få (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 67 i domen, och Peck mot Förenade kungariket, 28.1.2003, punkt 59 i domen). För att en begränsning av integritetsskyddet ska vara tillåten måste den grunda sig på lag, vara nödvändig i ett demokratiskt samhälle och stå i proportion till det eftersträvade målet. I rättspraxisen har till exempel ordningsstörningar, bekämpning av brottslighet och upprätthållande av den nationella säkerheten i allmänhet ansetts vara en godtagbar grund för till och med långtgående begränsningar av integritetsskyddet. Staten har också i vissa situationer en bred prövningsmarginal när det gäller vad som är nödvändigt, till exempel i fråga om upptagning av personuppgifter om personer som misstänks för terroristbrott (Segerstedt-Wiberg m.fl. mot Sverige, 6.6.2006, punkterna 87 och 88 i domen). Domstolen har också beaktat innehållet och förutsebarheten i lagstiftningen. För att en begränsande åtgärd ska vara förenlig med lagen förutsätts inte enbart att åtgärden grundar sig på lagen, utan den ska också vara tillgänglig för de registrerade personerna och dess konsekvenser ska vara förutsebara (Segerstedt-Wiberg m.fl. mot Sverige, 6.6.2006, punkt 76 i domen). Domstolen har konstaterat att artikel 8 kränkts bland annat för att det i den nationella lagstiftningen inte funnits bestämmelser om uppgifternas innehåll, förvaringstiden för uppgifterna och de persongrupper som det kan samlas in upp-

gifter om (se till exempel Europadomstolens dom i målet Rotaru mot Rumänien 4.5.2000, punkterna 45–63 i domen).

Grundlagsutskottet har upprepade gånger konstaterat att den gällande lagen om behandling av personuppgifter i polisens verksamhet är mycket komplicerad till såväl struktur som innehåll och att statsrådet har anledning att överväga en totalrevidering av lagen senast när det slutliga innehållet i den kommande EU-regleringen om datasekretess klarnar. Utskottet har understrukit att den konstitutionella granskningen av den kommande lagstiftningen kommer att göras utifrån lagstiftningshelheten. Polisens personregister innehåller mycket sådan information som det är synnerligen viktigt att skydda mot obehörig användning (GrUU 42/2014 rd, GrUU 18/2012 rd). Grundlagsutskottet har också uppmärksammat att datainnehållet ökat ytterligare i och med de bestämmelser som tidigare fogats till lagen. I sådana situationer måste användningen övervakas särskilt noga (GrUU 42/2014 vp). Lagförslag 1 och 2 i propositionen innebär till vissa delar en utökning av datainnehållet i de personregister som förs av polisen.

Lagförslagen gäller behandling av personuppgifter i polisens verksamhet och innebär till stor del åtgärder som begränsar integritetsskyddet. Om de allmänna förutsättningarna för de här begränsande åtgärderna föreskrivs det i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (RP /2018 rd) samt i EU:s allmänt tillämpliga dataskyddsförordning. För att vara godtagbara ska de begränsande åtgärderna vara förenliga både med kraven i den allmänna dataskyddslagstiftningen och med kraven i 10 § i grundlagen och i människorättskonventionerna på det sätt som framkommer av tolkningspraxisen. Av grundlagsutskottets tolkningspraxis framgår, utöver vad som är förenligt med människorättskonventionerna och vilka krav som det föreskrivs om i lag, även att begränsningar av grundläggande fri- och rättigheter ska vara exakta och noggrant avgränsade, godtagbara och proportionerliga och de får inte påverka kärnområdet för de grundläggande fri- och rättigheterna. Dessutom ska begränsningen av de grundläggande fri- och rättigheterna vara förenad med ett adekvat rättsskydd. (GrUU 21/2006 rd, s. 3, GrUU 20/2005 rd, GrUU 12/1998 rd, s. 3 och 6, GrUU 8/1995 rd, GrUB 25/1994 rd, s. 4–5). I likhet med Europadomstolens tolkningspraxis har grundlagsutskottet ansett att bestämmelserna i lagen överlag ska vara så pass exakta att de gör myndigheternas åtgärder tillräckligt förutsebara (GrUU 15/1996 rd). Det föreskrivs om uttryckliga inskränkningar av den registrerades rätt till insyn till den del som det är fråga om behandling av personuppgifter som anknyter till brottmål och den nationella säkerheten. I situationer som hör till dataskyddsförordningens tillämpningsområde ska inskränkningar i den registrerades rätt till insyn vara tillåtna endast i enskilda fall, om inskränkningen är proportionerlig.

I enlighet med EU:s dataskyddslagstiftning får personuppgifter inte behandlas mer än nödvändigt och obehövliga personuppgifter får inte behandlas (proportionalitetsprincipen). Personuppgifter får i regel behandlas endast för det ändamål som det föreskrivs om i lagen och som uppgifterna insamlades för (principen om ändamålsbundenhet). Grundlagsutskottet har betonat behovet av att säkerställa att principen om ändamålsbundenhet följs i behandlingen av personuppgifter (GrUU 20/2016 rd, GrUU 13/2016 rd, GrUU 21/2012 rd, GrUU 47/2010 rd och GrUU 25/2009 rd). Proportionalitetsprincipen och principen om ändamålsbundenhet kan anses uppfylla kraven i bestämmelserna om de grundläggande fri- och rättigheterna då den registrerades skydd för privatlivet begränsas endast i den mån som det är nödvändigt och i rätt proportion till det eftersträvade målet. Dataskyddslagstiftningen gör det ändå möjligt att behandla personuppgifter för något annat ändamål, om det föreskrivs om detta i lagen och behandlingen är nödvändig och proportionerlig. Trots detta begränsar EU:s dataskyddsdirektiv att personuppgifter lämnas ut till andra behöriga myndigheter än de som hör till direktivets tillämpningsområde också när de här myndigheterna sköter sina lagstadgade, offentliga uppgifter, om behandlingen av personuppgifter i samband med myndighetens uppgift inte som sådan hör till direktivets tillämpningsområde. Med beaktande av grundlagsutskottets tolkningspraxis måste

bestämmelserna också vara tillräckligt detaljerade och noggrant avgränsade. De här begränsningarna måste beaktas i bestämmelserna om både den ursprungliga och den förenliga behandlingen av personuppgifter och i bestämmelserna om utlämnande av personuppgifter.

I 2 kap. i lagförslag 1 föreskrivs det på samma sätt som i den gällande lagen om de ursprungliga ändamålen med behandlingen av personuppgifterna och de ersätter bestämmelserna om informationssystemet för polisärenden, informationssystemet för förvaltningsärenden och informationssystemet för misstänkta samt bestämmelserna om polisens övriga personregister. I lagen föreskrivs det också om förenlig behandling av personuppgifter. Bestämmelserna om förenlig behandling av personuppgifter och utlämnande av personuppgifter utvidgas och preciseras till vissa delar. Ett syfte med bestämmelserna är att slopa enskilda polisinrättningars register och tillfälliga register och ersätta dem med bestående, nationella register så långt det är möjligt, vilket bedöms underlätta övervakningen av registren och därmed förbättra de registrerades integritetsskydd och rättsskydd. Enligt grundlagsutskottet är en reglering tillräckligt noggrant avgränsad om de uppgifter som ska registreras i informationssystemen är tillräckligt noggrant specificerade (GrUU 51/2002 rd, s. 2, GrUU 18/2012 rd). Däremot är det enligt grundlagsutskottet problematiskt om det enligt bestämmelsens formulering i sista hand är myndigheten som i hög grad själv definierar innehållet i de personuppgifter som registreras (GrUU 18/2012 rd). Det ska föreskrivas om de personuppgifter som ska registreras på ett heltäckande och detaljerat sätt, men regleringstekniken skiljer sig från den gällande lagens. På samma sätt som i den gällande lagen ska det föreskrivas om förvaringstiden för personuppgifter separat för varje ändamål med behandlingen.

När det gäller observationsuppgifter föreslås det inga ändringar i förhållande till den gällande regleringen. Det föreslås däremot en separat paragraf för observationsuppgifterna. I fråga om observationsuppgifterna har grundlagsutskottet konstaterat att det handlar om en potentiellt mycket omfattande datamängd som berör privatlivet (GrUU 18/2012 rd). Observationsuppgifter är dessutom ofta av otillförlitligt slag och det finns risk för att oskyldiga stämplas. Utöver det som nämns ovan har grundlagsutskottet i fråga om behandlingen av uppgifter av detta slag påpekat behovet av att försäkra sig om att uppgifterna är exakta och tillförlitliga (GrUU 27/2006 rd, s. 2/II) och att till uppgifterna foga en bedömning av tillförlitligheten hos den som lämnat uppgifterna och uppgifternas riktighet (GrUU 51/2002 rd, s. 2/II). Dessutom får observationsuppgifter lagras under en rätt kort tid och då begränsar behandlingen av personuppgifter som till sin karaktär är obekräftade eller till sin betydelse otillförlitliga skyddet för privatlivet endast i den mån som det är nödvändigt för polisen att sköta sitt uppdrag. Om regleringen är preciserad på detta sätt i fråga om datainnehåll, användningsändamål och förvaringstid är den inte problematisk med avseende på skyddet för personuppgifter enligt grundlagsutskottet. Grundlagsutskottet har dock ansett att med tanke på observationsuppgifternas natur är det ändå viktigt att villkoren för lagring av uppgifter tolkas strikt och i synnerhet så att observationsuppgifter kan lagras endast om det finns misstanke om anknytning till kriminell verksamhet (GrUU 18/2012 rd).

Det föreslås att bestämmelsen om informationssystemet för misstänkta i den gällande lagen ska ersättas med en bestämmelse om behandlingen av personuppgifter som anknyter till kriminalunderrättelseinhämtning. Det som föreslås i 2 kap. 4 § innebär en utökning av registrets innehåll i fråga om både datainnehållet och de persongrupper som ska registreras. Även med tanke på tillämpningen av den här bestämmelsen bör kraven på proportionalitet och ändamålsbundenhet beaktas, då den registrerades skydd för privatlivet enligt dem endast får begränsas i den mån som det är nödvändigt och i rätt proportion till det eftersträvade målet. I bestämmelsen föreslås en precisering av de persongrupper som det får registreras och behandlas uppgifter om för ändamålet med behandlingen i fråga. I bestämmelsen har behandlingen av personuppgifter som anknyter till kriminalunderrättelseinhämtning med beaktande av grundlagsutskottets tidigare anmärkningar begränsats så att det i informationssystemet endast får registre-

ras uppgifter i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser kan bedömas ha samband med brottslig verksamhet. Då uppgifterna registreras ska det om möjligt bifogas en bedömning av uppgiftslämnarens eller källans tillförlitlighet och uppgifternas riktighet. Personuppgifter som anknyter till kriminalunderrättelseinhämtning får enligt den föreslagna paragrafen om förenlig behandling av personuppgifter inte användas för att fatta beslut eller lämna utlåtande om beviljande av ett tillstånd eller tillståndets giltighet, med hänsyn till deras potentiellt otillförlitliga karaktär.

I den föreslagna bestämmelsen om behandlingen av personuppgifter som anknyter till kriminalunderrättelseinhämtning har särskild uppmärksamhet fästs vid kriterierna för registrering och behandling av olika persongrupper vars personuppgifter det är nödvändigt för polisen att behandla med beaktande av kriminalunderrättelseinhämtningens karaktär. I bestämmelsen föreslås det en lägre tröskel för registrering och behandling till de delar som det handlar om personer med egentlig koppling till brottslig verksamhet. När det gäller personer som på olika sätt kopplas till brott har också Europadomstolen ansett att det för att utreda brott är godtagbart att registrera inte enbart personuppgifter om den som egentligen är misstänkt för brottet, utan också att registrera personuppgifter till exempel om dem som befann sig på platsen vid tidpunkten för gripandet. (Murray mot Förenade kungariket, 28.10.1994, punkt 93 i domen). I fråga om behandlingen av personuppgifter som anknyter till kriminalunderrättelseinhämtning föreslås det att bestämmelsen ska göra det möjligt att behandla uppgifter om personer med olika kopplingar till den brottsliga verksamheten, till exempel för att utreda sambanden mellan dem, inklusive kriminell bakgrund. Europadomstolen har däremot påpekat att urskillningslös och obegränsad behandling av uppgifter i ett brottsregister utan tydliga bestämmelser om rättsskyddsgarantierna, som behandlingskriterier och förvaringstider för uppgifterna och ändamålen med behandlingen, sannolikt strider mot artikel 8 i Europakonventionen (M.M. mot Förenade kungariket, 13.11.2012, punkt 199 i domen).

Dessutom bedöms att man i registret kan behöva anteckna till exempel vem den misstänktas våldshot är riktat mot eller kan riktas mot. Som motiv för detta förfarande har angetts att polisen inte annars vid behov kan skydda den som är målsägande, offer eller vittne. Enligt den föreslagna paragrafen ska de här personerna dock omfattas av en högre tröskel för behandlingen av personuppgifterna. Genom den högre behandlingströskeln säkerställs att för sådana registrerade vars ställning är klar begränsas skyddet för privatlivet endast i den mån som det är nödvändigt för att förhindra, avslöja eller utreda den förmodade brottsliga verksamheten. Rättsskyddsgarantierna för de här personerna måste också beaktas särskilt. Grundlagsutskottet har tidigare påpekat att också uppgifter om potentiella eller verkliga brottsoffer kan införas i informationssystemet för misstänkta som uppgifter som hänför sig till brottet enligt motiveringen till bestämmelsen. Den gällande lagens 4 § omfattar dock inte detta ändamål (GrUU 51/2002 rd). Det att registreringen av offrens namn i registret endast grundar sig på motiveringen till bestämmelsen kan inte betraktas som en noggrant avgränsad reglering i enlighet med grundlagsutskottets tolkningspraxis. För målsägande, offer, och vittnen i fråga om ett brott föreslås ett kriterium som framgår direkt av den föreslagna ordalydelsen i 4 § 3 mom.

I lagförslag 1 föreslås en ny bestämmelse (2 kap. 7 § 2 mom.) om behandling av personuppgifter som fåtts i samband med polisuppdrag för bedömning av om de är behövliga. Utifrån den föreslagna bestämmelsen får personuppgifter också registreras i polisens informationssystem om det krävs för bedömningen av uppgifternas betydelse. Eftersom det i det ögonblick som uppgifterna registreras är oklart om de är av betydelse med tanke på polisens uppdrag, begränsas inte de persongrupper som får behandlas för ändamålet i fråga i bestämmelsen. Först av resultatet av den behövlighetsbedömning som avses i bestämmelsen framgår det om det är fråga om personer som misstänks för delaktighet i brottslig verksamhet eller personer som annars är förknippade med brottet eller om utomstående personer. Bestämmelsen ska tillämpas både på behandlingen av personuppgifter som anknyter till brottmål och på behand-

lingen av personuppgifter som anknyter till upprätthållande av allmän ordning och säkerhet. Den föreslagna bestämmelsen innebär således en utökning av det datainnehåll och de persongrupper som ska lagras i polisens personregister i förhållande till den gällande regleringen. I den föreslagna bestämmelsen om bedömning av betydelsen ska proportionaliteten och ändamålsbundenheten beaktas på samma sätt som i förslaget om behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning. Vid bedömningen av om bestämmelserna är förenliga med grundlagen kan det också vara av betydelse om den straffrättsliga legalitetsprincipen i 8 § i grundlagen realiseras och kravet på rättsskydd i 21 § uppfylls. Med tanke på om en begränsning av integritetsskyddet är godtagbar är det av betydelse i vilket samband personuppgifterna har samlats in och för vilket ändamål de ska användas samt hurdana uppgifter det handlar om.

Europadomstolen har ansett att enbart det faktum att den registrerade är orolig för i vilket syfte de lagrade personuppgifterna kommer att användas samt om den registrerade har möjlighet att förhindra att personuppgifterna behandlas är av betydelse med avseende på begränsningen av integritetsskyddet (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 71 i domen, Rotaru mot Rumänien, 4.5.2000, punkt 46 i domen). Lagstiftningen måste också vara tillräckligt noggrant avgränsad för att trygga att en person kan förutse konsekvenserna av sina handlingar (Rotaru mot Rumänien, 4.5.2000, punkt 55 i domen, Malone mot Förenade kungariket, 2.8.1984, punkt 67 i domen, Amann mot Schweiz, 16.2.2000, punkt 56 i domen). Den föreslagna bestämmelsen innebär att även utomstående kan bli registrerade för ett behandlingsändamål. När Europadomstolen har konstaterat om myndigheternas förfarande varit godtagbart, har den i sin rättspraxis beaktat om till exempel fotografier som tagits i samband med demonstrationer och där det förekommer okända människor inte har registrerats i informationssystemet och att myndigheterna inte med hjälp av behandling av personuppgifter har försökt utreda de här personernas identitet (Friedl mot Österrike, 31.1.1995, utlåtande av kommissionen för mänskliga rättigheter, punkterna 49–51, P.G. och J.H. mot Förenade kungariket, 25.9.2001, punkt 58 i domen, S. och Marper mot Förenade kungariket, 4.12.2008, punkt 82 i domen). Vikt måste också fästas vid de eventuella risker för att bli stämplad som hör samman med principen om oskyldighetspresumtion (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 122 i domen).

I EU:s dataskyddsförordning och dataskyddsdirektiv finns bestämmelser om behandling av känsliga personuppgifter och i dem ställs strängare krav än tidigare för behandlingen av de här uppgifterna, inklusive krav om skydd för känsliga personuppgifter. I den föreslagna bestämmelsen om behandling av känsliga personuppgifter har de här kraven beaktats. Grundlagsutskottet har till exempel fäst uppmärksamhet vid att behandlingen av känsliga uppgifter tangerar kärnan i skyddet för personuppgifter inom privatlivet och därför måste bestämmelser som tillåter behandling av sådana uppgifter vara exakta (GrUU 25/1998 rd, s. 3, GrUU 51/2002 rd). Grundlagsutskottet har också ansett att det i lagen måste tas in exakta bestämmelser om behörighet att behandla känsliga uppgifter när det gäller polisens behandling av personuppgifter, eftersom personuppgiftslagen, som är en allmän lag, inte ger sådan behörighet (GrUU 51/2002 rd). I EU:s nya dataskyddslagstiftning utvidgas definitionen av känsliga personuppgifter till att innefatta också genetiska uppgifter och biometriska uppgifter som polisen med stöd av den gällande lagstiftningen behandlar i form av signalement (DNA-spår, fingeravtryck och ansiktsbilder) och i samband med tillståndsärenden (fingeravtryck och ansiktsbilder). I den gällande personuppgiftslagen anges inte dessa uttryckligen som känsliga personuppgifter. I praktiken ska dock DNA-spår redan i nuläget behandlas som känsliga personuppgifter i sådana situationer där de ger information om en persons ras eller etniska ursprung, hälsotillstånd eller sjukdom. Det bör påpekas att det i dataskyddsdirektivet, som tillämpas på brottmål, krävs högre behandlingströskel för behandlingen av känsliga personuppgifter än för behandlingen av andra personuppgifter. Denna ändring i förhållande till den gällande lagen är betydelsefull som en faktor som höjer integritetsskyddet i synnerhet när det handlar om fingeravtryck och

ansiktsbilder som behandlas i flera informationssystem, vilket möjliggör en omfattande behandling av personuppgifterna. Polisen behandlar biometriska personuppgifter också för andra ändamål, såsom ansökningar om pass och identitetskort, men till denna del betonas ingen behandlingströskel i EU:s nya dataskyddsförordning, vilket också har beaktats i 2 kap. 2 § i lagförslag 1. Behandlingen av känsliga personuppgifter måste till denna del dock bindas till skötseln av en för polisen lagstadgad uppgift.

Med beaktande av att behandlingströskeln i dataskyddsdirektivet är högre än tidigare vad gäller biometriska och genetiska uppgifter är de viktigaste förslagen med tanke på respekten för privatlivet och skyddet för personuppgifter de föreslagna bestämmelserna om registreringen och behandlingen av biometriska uppgifter och DNA-uppgifter i brottmål. I 2 kap. 11 § 5 mom. i lagförslag 1 föreslås också en utvidgning i förhållande till den gällande lagen, då fingeravtryck som har samlats in med stöd av 131 § i utlänningslagen ska kunna användas för förebyggande, avslöjande och utredning av terroristbrott eller andra grova brott. Förslaget innebär en inskränkning i skyddet för privatlivet för de personer som registrerats i enlighet med utlänningslagen. Användningen av fingeravtryck för andra ändamål än de ursprungliga ändamålen med behandlingen avgränsas dock till grova brott som jämställs med brott enligt Eurodacförordningen och dessutom ska användningen vara nödvändig. Den föreslagna utvidgningen bedöms närmare nedan med tanke på hur skyddet för privatlivet och jämlikhetsprincipen realiseras i enlighet med grundlagen.

Europadomstolen har konstaterat att till exempel fingeravtryck innehåller sådan information om en individ som gör det möjligt att exakt identifiera honom eller henne i mycket varierande sammanhang (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 84 i domen). Grundlagsutskottet har redan tidigare bedömt att sådana biometriska identifieringsuppgifter i många avseenden kan jämställas med känsliga uppgifter. Att tillåta behandling av känsliga uppgifter berör själva kärnan i skyddet för personuppgifter som hör till privatlivet (GrUU 29/2016 rd, GrUU 37/2013 rd, s. 2/I). På grund av detta kan redan införandet av fingeravtrycksuppgifter i ett sådant register ge anledning till oro med tanke på skyddet för privatlivet (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 85 i domen). Också EU-domstolen har ansett att tagande och registrering av fingeravtryck ingriper i respekten för privatlivet och skyddet för personuppgifter i artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (Schwarz mot Stadt Bochum C- 291/12, punkt 30 i domen). (Se även GrUU 29/2016 rd, GrUU 13/2016 rd.) Enligt grundlagsutskottets uppfattning är det betydelsefullt att allvarliga risker som gäller informationssäkerhet och missbruk av uppgifter kan vara förknippade med omfattande databaser med biometriska kännetecken och i sista hand kan de utgöra ett hot mot någons identitet (GrUU 29/2016 rd, GrUU 13/2016 rd, s. 4, på finska, GrUU 14/2009 rd, s. 3/I). Utskottet har ansett att inrättandet av ett sådant register måste bedömas med avseende på villkoren för begränsning av de grundläggande fri- och rättigheterna, särskilt med avseende på om en sådan begränsning är godtagbar och uppfyller kravet på proportionalitet (GrUU 29/2016 rd, GrUU 21/2012 rd, GrUU 47/2010 rd och GrUU 14/2009 rd). Europadomstolen har konstaterat att Europakonventionen kränkts då särskilda rättsskyddgarantier har saknats för insamling, förvaring och utplåning av fingeravtryck i de fall då det varit fråga om brottsmisstänkta som inte dömts för brott (M.K. mot Frankrike, punkt 26 i domen). Motsvarande principer måste tillämpas på den reglering som gäller behandlingen av DNA-uppgifter.

Ställningstaganden om EU:s dataskyddslagstiftning och stadga om de grundläggande rättigheterna samt grundlagsutskottets ställningstaganden beaktas genom bestämmelser som kompletterar de allmänna dataskyddsbestämmelserna och med hjälp av vilka behandlingen av känsliga personuppgifter i brottmål begränsas till nivån för nödvändighetskriteriet, och genom bestämmelser som gäller skydd av behandlingen av känsliga personuppgifter. Enbart en hänvisningsbestämmelse om tillämpningsområdet anses inte tillräcklig, utan genom kompletterande bestämmelser är det meningen att säkerställa att de nya, strängare kraven följs också i

polisens behandling av personuppgifter. Utplåningsbestämmelserna hör också till rättsskyddsgarantierna. Europadomstolen har påpekat att förvaringstiderna ska vara proportionella med tanke på ändamålet med behandlingen av personuppgifterna och att förvaringstiderna måste begränsas (S. och Marper mot Förenade kungariket, punkterna 107 och 108 i domen). Det bedöms att de föreslagna bestämmelserna uppfyller de krav som framgår av grundlagsutskottets tolkningspraxis.

Den registrerades rätt till insyn är med tanke på integritetsskyddet särskilt viktig för de personuppgifter som ska behandlas. Huvudreglerna för den registrerades rätt till insyn finns i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (RP /2018 rd) och i EU:s dataskyddsförordning, men i kap. 6 i lagförslag 1 föreskrivs det om inskränkningar i den registrerades rätt till insyn. Bakom inskränkningen av privatlivet ska det finnas ett godtagbart samhälleligt intresse och inskränkningen ska stå i proportion till det eftersträvade målet. Detta betyder att inskränkningarna måste vara nödvändiga för att uppnå ett godtagbart mål. Det är tillåtet att begränsa en grundläggande fri- eller rättighet endast om målet inte kan uppnås på ett sätt som inte ingriper lika mycket i den grundläggande fri- eller rättigheten. En inskränkning får inte heller vara mer genomgripande än vad som är motiverat med hänsyn till hur tungt vägande det bakomliggande samhälleliga intresset är i relation till det skyddsintresse som ska inskränkas (se GrUB 25/1994 rd, s. 5/I–II och till exempel GrUU 56/2014 rd, s. 3/I–II och GrUU 18/2013 rd, s. 2). När det gäller brottmål motsvarar de uttryckliga inskränkningarna av den registrerades rättigheter i regel den gällande lagen, men utöver dessa föreslås begränsningar i fråga om de nya ändamålen med behandlingen av personuppgifter som anknyter till kriminalunderrättelseinhämtning och bedömningen av om personuppgifterna är behövliga. Det ska inte finnas någon rätt till insyn i personuppgifter som behandlas av Skyddspolisen, vilket motsvarar den gällande lagstiftningen. Begränsningarna i lagförslag 1 anknyter således dels till förebyggande, avslöjande och utredning av brott, dels till tryggande av den nationella säkerheten. Dessa har i Europadomstolens, EU-domstolens och högsta domstolens rättspraxis betraktats som sådana tungt vägande samhälleliga intressen, vars mål inte kan uppnås på ett sätt som inte ingriper lika mycket i den grundläggande fri- eller rättigheten. Vid behandlingen av personuppgifter som hör till dataskyddsförordningens tillämpningsområde (2 kap. 9 §) kan den registrerades rättigheter endast begränsas i enskilda fall, om det enligt villkoren i artikel 23.1 i dataskyddsförordningen är en nödvändig och proportionell åtgärd. Den registrerade fråntas inte heller helt möjligheten att övervaka behandlingen av sina personuppgifter, utan i situationer där det förekommer begränsningar kan han eller hon utöva sin rätt indirekt via dataskyddsmyndigheten. Begränsningarna går således inte längre än vad som är nödvändigt för att uppnå målet.

Utlämnande av personuppgifter

På samma sätt som i den gällande lagen finns det i lagförslaget (4 kap.) också bestämmelser om utlämnande av personuppgifter till andra myndigheter, brottsbekämpande myndigheter i Europeiska unionens medlemsstater och informationssystem som omfattar EU samt till tredjeländer och internationella organisationer. Däremot föreskrivs det inte om utlämnande av personuppgifter mellan polisens enheter, utan behandlingen av personuppgifter grundar sig till denna del också på ändamålen med behandlingen av personuppgifterna och ett enskilt ändamål ska alltid hänföra sig till en särskild polisuppgift. I 4 kap. 1 och 2 § i lagförslag 1 finns en detaljerad förteckning över de myndigheter som polisen trots sekretessbestämmelserna har rätt att lämna ut uppgifter till genom teknisk anslutning eller som en datamängd. Även i lagförslag 2 föreskrivs det detaljerat om situationer då personuppgifter får lämnas ut i enlighet med PNR-direktivet.

EU:s nya dataskyddslagstiftning och bestämmelser om grundläggande rättigheter sätter gränser för bestämmelserna om utlämnande av uppgifter. Med tanke på bestämmelserna om grund-

läggande rättigheter är principen i skäl 22 i ingressen till dataskyddsdirektivet betydelsefull. Enligt detta skäl bör offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, till exempel skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning i allmänhetens intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut bör alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser om dataskydd som är tillämpliga på behandlingens ändamål. I de bestämmelser i lagförslag 1 som gäller utlämnande av personuppgifter till andra myndigheter i enskilda fall har det för det första beaktats att polisen kan behöva lämna ut personuppgifter till en annan myndighet trots sekretessbestämmelserna i syfte att förebygga, avslöja eller utreda brott och för det andra att samma uppgifter i samband med att ärendet utreds kan visa sig vara viktiga för att en annan myndighet ska kunna utföra sina lagstadgade uppgifter. Fastän polisen när de utreder ett ärende kan komma fram till att det inte finns skäl att misstänka brott, kan den handling som ursprungligen misstänktes vara ett brott uppfylla kriterierna för en administrativ förseelse. Utredning av administrativa förseelser bör betraktas som behandling av personuppgifter som är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in, med beaktande av det i rättspraxisen etablerade förbudet mot dubbla straff (ne bis in idem-principen).

Grundlagsutskottet har i sin praxis ansett att det i fråga om sådan rätt att få uppgifter som går före sekretessbestämmelserna i sista hand är fråga om att den myndighet som har rätt att få uppgifterna med sina egna behov åsidosätter de grunder och intressen som skyddas genom tystnadsplikt hos den myndighet som innehar uppgifterna. Grundlagsutskottet har ansett att det viktiga för skyddet för privatlivet är att användning av sekretessbelagda personuppgifter och röjande av uppgifter i strid med registrets syfte är straffbara gärningar enligt strafflagen, lagen om offentlighet i myndigheternas verksamhet och personuppgiftslagen (GrUU 4/2014 rd s. 4, GrUU 39/2009 rd, s. 3). Det bedöms att de föreslagna bestämmelserna om utlämnande av uppgifter inte utgör något problem i grundlagshänseende. I de bestämmelser som gäller utlämnande av uppgifter till andra myndigheter har man försökt försäkra sig om att kriteriet för utlämnande av uppgifter, på motsvarande sätt som i den gällande lagstiftningen om behandling av personuppgifter, är att behandlingen av personuppgifterna är nödvändig dels för att förebygga, avslöja eller utreda brott, dels för att en behörig myndighet ska kunna utföra sin lagstadgade uppgift, så att uppgifter får lämnas ut för ändamål som är förenliga med personregistrets användningsändamål. Grundlagsutskottet har beaktat bland annat hur rätten att få uppgifter är kopplad till nödvändighetskriteriet. Rätten att få uppgifter och möjligheten att lämna ut uppgifter har kunnat gälla behövliga uppgifter för ett visst syfte, om lagen ger en uttömmande förteckning över uppgiftsinnehållet. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att uppgifterna är nödvändiga för ett visst syfte (GrUU 19/2012 rd, s. 3–5, GrUU 62/2010 rd, s. 4/I). Kriterierna som gäller rätten att få personuppgifter ändras inte väsentligt i och med att EU:s nya dataskyddslagstiftning träder i kraft. Vid beredningen av lagförslagen har man försökt beakta motiveringarna i EU:s dataskyddslagstiftning om vad som ska anses som förenlig behandling av personuppgifter.

Ju mer generell den lagstiftning som ger rätt att få uppgifter är, desto större är faran att sådana intressen kan åsidosättas mycket automatiskt. Ju fullständigare bestämmelserna kopplar rätten till information till materiella villkor, desto sannolikare är det att begäran om information måste motiveras i praktiken. Då kan också den som lämnar ut informationen bedöma begäran mot de lagliga villkoren för utlämnandet. Detta har beaktats genom en justering av bestämmelserna om den tekniska anslutningen. Genom att vägra lämna ut informationen kan den som

innehar den få till stånd en situation där en utomstående myndighet måste pröva skyldigheten att lämna ut information, det vill säga tolka bestämmelserna. Denna möjlighet är viktig då det gäller att anpassa tillgången till information och sekretessintressena till varandra (GrUU 62/2010 rd, s. 3–4, GrUU 42/2010 rd, s. 3). I praktiken har polisen med stöd av polislagen omfattande befogenheter att få information och de här befogenheterna har bedömts innefatta också rätten att i enskilda fall få de personuppgifter som behövs för utförandet av en polisuppgift. Det föreskrivs om polisens rätt att få personuppgifter genom teknisk anslutning eller som en datamängd i 3 kap. i lagförslaget på motsvarande sätt som i den gällande lagstiftningen.

EU:s gällande dataskyddsrambeslut gör det möjligt att lämna ut personuppgifter direkt till privata sammanslutningar eller näringsidkare inom EU. I det nya dataskyddsdirektivet finns ingen direkt motsvarande bestämmelse, men till denna del inte heller någon särskild begränsande bestämmelse. Enligt artikel 8.1 i direktivet ska behandling av personuppgifter vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 i direktivet och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt. Enligt artikel 8.2 ska lagstiftningen åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål. I 4 kap. i lagförslag 1 föreslås det bestämmelser som gör det möjligt att i begränsade situationer lämna ut personuppgifter till privata sammanslutningar och personer om utlämnandet är nödvändigt för att polisen ska kunna utföra sina uppdrag och det inte är möjligt för polisen att utföra sina uppdrag utan inskränkningar i integritetsskyddet. Regleringen motsvarar bestämmelserna i den gällande lagen, förutom det som föreslås i 4 kap. 3 § 1 mom., som gör det möjligt att lämna ut uppgifter i situationer då detta är nödvändigt på grund av att saken är brådskande, att det är fråga om en farosituation, för att brott ska kunna förebyggas, egendom ska kunna återställas till ägaren eller av skäl som har samband med utredningen och utlämnandet av uppgifterna inte strider mot den registrerades legitima intresse. Bestämmelsen motsvarar till sitt ändamål artikel 29 i dataskyddsdirektivet, som gör det möjligt att lämna ut personuppgifter till enskilda i noggrant avgränsade situationer. Med beaktande av de föreslagna avgränsningarna i bestämmelsen bedöms att förslaget uppfyller grundlagens krav på proportionalitet i bestämmelserna. Det innebär inte heller ett sådant undantag från principen om ändamålsbundenhet som går längre än vad som är nödvändigt för att uppnå målet.

Dessutom föreslås i 4 kap. 4 § i lagförslag 1 en ny bestämmelse om utlämnande av personuppgifter i anknytning till giltigheten av tillstånd till sådana privata sammanslutningar eller näringsidkare som i någon annan lag har ålagts sådana uppgifter som nödvändigt kräver behandling av uppgifter om ett tillstånds giltighet för att kunna utföras. Bestämmelsen innefattar alla tillståndsärenden som polisen handlägger och lämnar det öppet till vilka privata sammanslutningar och näringsidkare som personuppgifter får lämnas ut. Dessa preciseras först när det föreskrivs om detta någon annanstans i lag. Däremot är rätten att lämna ut uppgifter i paragrafen avgränsad endast till uppgifter om tillståndets giltighet och därför bedöms bestämmelsen till den delen uppfylla kravet på noggrann avgränsning i behandlingen av personuppgifter. Andra personuppgifter får inte med stöd av paragrafen lämnas ut genom elektroniska tjänster. Dessutom avgränsas sättet att lämna ut uppgifter så att uppgifter endast får lämnas ut som enskilda sökningar. Syftet med den föreslagna avgränsningen är att begränsa ingripandet i integritetsskyddet till vad som är nödvändigt för att den privata sammanslutningen eller näringsidkaren ska kunna utföra sin uppgift.

Med beaktande av grundlagsutskottets tolkning föreskrivs det i lagförslaget också under vilka förutsättningar personuppgifter får lämnas ut till ett tredjeland eller en internationell organisation. När det gäller polisens rätt att lämna ut uppgifter till internationella organisationer handlar det i praktiken om Interpol, som i ingressen till dataskyddsdirektivet jämställs med internationella organisationer. När personuppgifter lämnas ut ur polisens personregister till en behörig

myndighet i en främmande stat ska det enligt EU:s nya dataskyddslagstiftning handla antingen om ett ändamål med behandlingen som motsvarar det ursprungliga ändamålet eller om behandling av personuppgifter som är förenlig med registrets användningsändamål, om det föreskrivs om detta separat i den nationella lagstiftningen eller EU-lagstiftningen. I fråga om lagstiftning om utlämnande av personuppgifter till aktörer i länder utanför Europeiska unionen och Europeiska ekonomiska samarbetsområdet har grundlagsutskottet i sin vedertagna praxis hänvisat till artikel 25 i Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, enligt vilken en förutsättning för att personuppgifter ska få överföras är att ett tredjeland säkerställer en adekvat skyddsnivå med tanke på direktivet. Nivåkravet kan också härledas från 10 § 1 mom. i grundlagen. Grundlagsutskottet har i sin tidigare praxis ansett att det är skäl att i lagen ta in hänvisningar till direktivets och personuppgiftslagens bestämmelser om utlämnande av uppgifter. I dem finns bland annat de bestämmelser som ska tillämpas på överföring av uppgifter till tredjeländer (GrUU 2/2008 rd, s. 3, GrUU 43/2006 rd, s. 4, GrUU 51/2002 rd, s. 3, GrUU 14/2002 rd, s. 5). De här ersätts nu med nya bestämmelser som finns i kapitel V i dataskyddsförordningen och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten genom vilken dataskyddsdirektivet genomförs. Kommissionen får till skillnad från tidigare fastställa den adekvata dataskyddsnivån för behandlingen av personuppgifter som anknyter till brottmål. En adekvat dataskyddsnivå kan också grunda sig på andra rättsligt bindande garantier. Personuppgifter får lämnas ut utan dessa garantier endast i undantagsfall. De här bestämmelserna finns också i förslaget till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (RP /2018 rd). I och med dataskyddsdirektivet blir den personuppgiftsansvariges ansvar och kraven på övervakning av behandlingen av personuppgifter, som för närvarande grundar sig på personuppgiftslagen, mer framträdande än tidigare.

Kravet på att bestämmelser ska utfärdas genom lag gäller också möjligheten att lämna ut personuppgifter genom en teknisk anslutning. Grundlagsutskottet har ansett att det är nödvändigt att ställa kravet att den som begär uppgifter ska lägga fram en utredning om behörigt skydd för uppgifterna innan en teknisk anslutning öppnas (GrUU 12/2002 rd, s. 5). Grundlagsutskottet har ansett kravet vara nödvändigt bland annat för att den registeransvarige (numera den personuppgiftsansvarige) kan handla i enlighet med sina skyldigheter som är baserade på 32 § i personuppgiftslagen. Grundlagsutskottet har dock konstaterat att regleringen samtidigt avslöjar att en påfallande del av de omständigheter som sammanhänger med mottagande och utlämnande av uppgifter, inklusive i sista hand tolkningen av de bakomliggande bestämmelserna, i betydande grad blir beroende av praxis mellan parterna. Det är till exempel fråga om på vilket sätt omständigheter som enligt lagen faller utanför rätten att få uppgifter i själva verket inte lämnas ut via den tekniska anslutningen samt hur det i lagen eventuellt föreskrivna nödvändighetskriteriet eller andra kriterier i enskilda fall konstateras. Ansvarsfrågorna kan också vara problematiska (GrUU 14/2002 rd, s. 5–6).

I bestämmelserna om utlämnande av personuppgifter i lagförslag 1 har man försökt beakta grundlagsutskottets anmärkningar på ett bättre sätt än tidigare. I polisens gällande personuppgiftslag har uttrycket teknisk anslutning använts också på annat sätt än i sin egentliga betydelse. I fråga om informationssystemet för misstänkta är den tekniska anslutningen i den gällande lagen strängt avgränsad vad gäller de användare inom polisens personal som har rätt att använda teknisk anslutning. För de andra informationssystemen föreskrivs det om teknisk anslutning endast i de bestämmelser som gäller utlämnande av uppgifter och rätt att få uppgifter. Som metod för utlämnande av information och åtgärd som begränsar integritetsskyddet går teknisk anslutning inte längre än vad ett utlämnande som grundar sig på en separat begäran om uppgifter gör. Den personuppgiftsansvarige ska ansvara för att säkerställa att personuppgifterna är tillbörligt skyddade oberoende av det sätt som de lämnas ut på. Det föreslås att det i lagen, på samma sätt som i den gällande lagen, ska finnas detaljerade bestämmelser om till

vilka myndigheter och för vilka ändamål med behandlingen som personuppgifter får lämnas ut. För att den personuppgiftsansvariges övervakningsansvar ska realiseras måste den personuppgiftsansvarige även i fortsättningen separat bedöma under vilka förutsättningar som en teknisk anslutning får öppnas och då kan den personuppgiftsansvarige också bekräfta ansvarsfrågorna genom ett organisationstillstånd eller ett avtal. I de situationer när polisen behöver lämna ut personuppgifter i enskilda fall utan teknisk anslutning, föreslås utlämnandet av personuppgifter bindas till vad som är nödvändigt. Däremot föreslås det inte att bestämmelserna binds till polisens enskilda personregister ur vilka personuppgifter ska lämnas ut. De föreslagna bestämmelserna bedöms svara mot kravet i bestämmelserna om de grundläggande fri- och rättigheterna på att begränsningar av integritetsskyddet ska vara nödvändiga och proportionerliga.

Utöver teknisk anslutning kan polisen söka träffar i registrens referensuppgifter. Sådan sökning är i regel betydelsefull med tanke på skyddet för personuppgifter och skyddet för privatlivet, som båda tryggas i 10 § 1 mom. i grundlagen, i synnerhet med beaktande av att känsliga personuppgifter, såsom fingeravtrycksuppgifter och DNA-uppgifter, kan lämnas ut ur registren. Genom lagförslag 1 genomförs Prümfördraget och Prümrådsbeslutet på samma sätt som i den gällande lagen. Till informationsutbytet i enlighet med dem hör tre system för informationsutbyte som baserar sig på decentraliserad sökning (fordonsregisteruppgifter, fingeravtryck och DNA-spår). Grundlagsutskottet har tidigare tagit ställning till de här systemen (GrUU 56/2006 rd).

De system för sökning som polisen använder ger inte någon självständig befogenhet att samla in eller lagra uppgifter ur andra medlemsstaters register, utan befogenheten att lämna ut personuppgifter som är föremål för sökning i ett register bestäms i enlighet med respektive medlemsstats nationella lagstiftning. När det gäller skyddet för personuppgifter är det dessutom viktigt att polisen endast har tillgång till sådana fordons-, DNA- och fingeravtrycksregisters referensuppgifter som inte direkt kan kombineras med någon enskild person. Det är alltid polisen som prövar om personuppgifter ska lämnas ut. Grundlagsutskottet har inte ansett att de fördragsbestämmelser som anknyter till informationssökning i polisens personregister med signalement är problematiska med avseende på grundlagens 7 och 10 § (GrUU 56/2006 rd, s. 4). Även i Prümbesluten som ersatte Prümfördraget var system för att söka träffar baserade på decentraliserad informationssökning fortsättningsvis giltiga. Däremot har Europadomstolen ansett att modern, vetenskaplig teknologi för brottsprocesser inte får användas på vilka grunder som helst utan att fördelarna med sådan teknologi noggrant vägs mot deras konsekvenser för skyddet för privatlivet (S. och Marper mot Förenade kungariket, punkt 112 i domen). Grundlagsutskottet har även nyligen tagit ställning till en centraliserad teknologisk lösning för denna form av behandling av personuppgifter och påpekat att ett centraliserat system skulle innebära ett särskilt behov att se till att de personuppgifter som registreras i systemet skyddas mot farorna för missbruk och all olaglig tillgång till och användning av uppgifter (GrUU 29/2016 rd, se också Schrems C-362/14, punkt 91, Digital Rights Ireland C-293/12 och C-594/12, punkterna 54 och 55). Även övervakningen av behandlingen av personuppgifter och logguppgifter i anslutning till informationssökning måste emellertid ske i enlighet med lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. I de föreslagna bestämmelserna bevaras informationsutbyte som anknyter till Prümfördraget och Prümrådsbeslutet i sin nuvarande form för att säkerställa att EU-lagstiftningen genomförs korrekt. Det föreslås inte att bestämmelserna till denna del ska gå längre än vad som är nödvändigt för genomförandet. I bestämmelserna förtydligas dock vilka bestämmelser som ska tillämpas på informationsutbyte efter en träff i ett register. De föreslagna bestämmelserna innebär ingen inskränkning av integritetsskyddet i förhållande till EU-lagstiftningen.

PNR-direktivet

Den behandling av passageraruppgifter som avses i lagförslag 2 innebär också en begränsning av skyddet för privatlivet och skyddet för personuppgifter. Genom lagförslaget genomförs EU:s PNR-direktiv. Grundlagsutskottet har konstaterat att det inte ingår i dess konstitutionella uppgifter att bedöma regleringen av den nationella verkställigheten med avseende på den materiella EU-rätten (GrUU 51/2014 rd). Enligt grundlagsutskottet är det ändå viktigt att det i den mån som EU-lagstiftningen kräver reglering på det nationella planet eller möjliggör sådan tas hänsyn till de krav som de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ställer när det nationella handlingsutrymmet utnyttjas (se även GrUU 44/2016 rd, s. 4, GrUU 51/2014 rd, s. 2/II och de utlåtanden som det hänvisas till i dem). Enligt grundlagsutskottet förutsätter detta att statsrådets uppfattning om ramarna för det nationella handlingsutrymmet på lämpligt sätt klargörs i regeringens proposition (se även GrUU 44/2016 rd, s. 4).

I artikel 1.1 a i PNR-direktivet åläggs medlemsstaterna skyldigheten att tillämpa direktivet på överföring av passageraruppgiftssamlingar på flygningar utanför EU. I artikel 1.2 begränsas användningen av uppgifter som samlats in i enlighet med direktivet till att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Av artikel 2 framgår att en medlemsstat kan tillämpa PNR-direktivet på flygningar inom EU, antingen på alla eller endast valda flygningar inom EU, och därmed lämna tillämpningen i fråga om flygningar inom EU för nationell prövning. Direktivets tillämpningsområde är begränsat endast till lufttrafikföretag. Enligt gällande lydelse i 3 kap. 13 § 1 mom. 16 punkten i lagen om behandling av personuppgifter i polisens verksamhet har polisen redan nu rätt att få uppgifter av samfund och sammanslutningar ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott, för överlämnande till åtalsprövning samt för att nå efterlysta personer. Men till skillnad från direktivet gäller den gällande bestämmelsen alla transportörer och gör det redan för närvarande möjligt att lämna ut uppgifter genom teknisk anslutning eller som en datamängd. Däremot gäller den gällande bestämmelsen endast överföring av passageraruppgifter i enskilda fall och transportörerna är inte skyldiga att överföra passagerarförteckningar systematiskt och i stor skala.

Enligt lagförslag 2 ska ett lufttrafikföretag överföra de uppgifter som avses i den föreslagna paragrafens 1 mom. i regel för alla ankommande och avgående flygningar utanför eller inom Europeiska unionen. Den föreslagna enheten för passagerarinformation får behandla passageraruppgifter för identifiering av personer som kan vara delaktiga i terroristbrott eller grov brottslighet. I praktiken innebär genomförandet av direktivet att passageraruppgifter behandlas i stor skala och när personuppgifter lämnas ut till enheten begränsas de inte enbart till personer som misstänks vara delaktiga i brottslig verksamhet, utan gäller de personuppgifter som alla passagerare uppgett till flygbolaget i samband med biljettbokningen. I lagförslaget preciseras de personuppgifter som lufttrafikföretagen måste lämna ut till enheten för passagerarinformation om ankommande och avgående flygningar utanför eller inom Europeiska unionen. Passageraruppgifter ska få lagras under fem år i det personregister som förs av polisen, men uppgifterna måste maskeras när sex månader har förflutit sedan de mottogs. I lagförslaget höjs integritetsskyddet i enlighet med direktivet dessutom genom det att jämförelse av personuppgifter med polisens andra personregister begränsas till att gälla förebyggande, avslöjande och utredande av terroristbrott och annan grov brottslighet och att endast den enhet som inrättats för ändamålet och en tjänsteman som särskilt utsetts för detta har rätt att jämföra personuppgifter. Passageraruppgifter som lagrats i polisens personregister får inte användas för andra ändamål. I lagförslaget finns också en begränsning av behandlingen av känsliga personuppgifter.

För det första innebär bestämmelsen i 3 kap. 1 § 1 mom. 16 punkten i lagförslag 1, som motsvarar den gällande bestämmelsen, en utvidgning av tillämpningsområdet i förhållande till PNR-direktivet, vilket har betydelse med tanke på skyddet för privatlivet. PNR-direktivet på-

verkar inte medlemsstaternas möjligheter att i enlighet med nationell rätt tillhandahålla ett system för insamling och behandling av PNR-uppgifter från ekonomiska aktörer som inte är transportörer, till exempel resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka de samlar in och behandlar PNR-uppgifter, eller från andra transportföretag än de som anges i direktivet, förutsatt att sådan nationell rätt är förenlig med unionsrätten. Det föreslås ingen ändring i den gällande bestämmelsen som godkänts med grundlagsutskottets medverkan. Däremot utvidgas bestämmelserna enligt lagförslag 2 i och med genomförandet av direktivet, i synnerhet när det gäller de uppgifter som lufttrafikföretagen ska överföra. Grundlagsutskottet påpekade i samband med behandlingen av den gällande bestämmelsen att den bestämmelse som redan då föreslogs var vag till följd av paragrafens inledande stycke och ansåg att det är motiverat att precisera början på den föreslagna 16 punkten så att den gäller uppgifter som behövs "för att förhindra, avslöja, utreda och till åtalsprövning överlämna terroristbrott och allvarlig gränsöverskridande brottslighet". Bestämmelsens tillämpningsområde är dock i någon mån bredare och polisen har rätt att ta emot information om passagerare och personal ur register för att förhindra, avslöja och utreda brott och föra brott till åtalsprövning samt för att nå efterlysta personer. Däremot har grundlagsutskottet uppmärksammat att den rätt som fogats till den gällande lagen i sig är relativt begränsad, och den gäller bara polisens rätt att få vissa uppgifter genom en teknisk anslutning. Behandlingen av uppgifterna regleras av andra bestämmelser i lagen om behandling av personuppgifter i polisens verksamhet. Något som enligt grundlagsutskottet också är viktigt med avseende på skyddet för personuppgifter enligt 10 § 1 mom. i grundlagen är att uppgifterna inte ska bilda ett eget personregister och att bara en särskild enhet för passageraruppgifter kommer att ha åtkomsträtten till de mottagna uppgifterna (GrUU 42/2014 rd).

För det andra innebär lagförslag 2 en inskränkning av skyddet för privatlivet jämfört med nuläget i lagstiftningen. Till skillnad från de gällande bestämmelserna innebär genomförandet av direktivet att ett nytt personregister ska inrättas. I direktivet förutsätts dock att ett nytt register inrättas för lagring av passageraruppgifterna och för denna del ger direktivet medlemsstaterna inget handlingsutrymme. I lagförslaget finns detaljerade bestämmelser om behandlingen av passageraruppgifter och utlämnandet av dem till polisens andra enheter, behöriga myndigheter, Europol och tredjeländer i syfte att förebygga, avslöja eller utreda brott. Direktivet verkar inte heller ge lagstiftaren handlingsutrymme i fråga om vilken form av brottsbekämpning lagstiftningen ska gälla, varför lagförslaget avgränsas till att gälla terroristbrott och andra grova brott. Direktivet ger dock den nationella lagstiftaren handlingsutrymme i fråga om vilka nationella register som i direktiven avses som väsentliga databaser för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och som passageraruppgifterna ska jämföras med. Det föreslås att enheten för passagerarinformation ska få omfattande rätt att genom automatiserade metoder jämföra passageraruppgifter som den tagit emot med uppgifter som lagrats i syfte att trygga de behöriga myndigheternas brottsutredning och kriminalunderrättelseinhämtning samt rätts- och samhällsordningen och att upprätthålla allmän ordning och säkerhet, de personuppgifter som avses i 7 kap. 3 § i lagförslag 1 och som behandlas av skyddspolisen samt de uppgifter som lagrats i det i 1 kap. 3 § 2 punkten i lagförslag 1 avsedda Schengens informationssystems och den internationella kriminalpolisorganisationens (I.C.P.O.-Interpol) databaser. Bestämmelsen omfattar i regel utan begränsningar alla de databaser som används för sådana ändamål med behandlingen som anknyter till brottmål och till upprätthållande av allmän ordning och säkerhet i 2 kap. i lagförslag 1. Med tanke på begränsningen av skyddet för privatlivet är det också av betydelse hurdant datainnehåll de här databaserna innehåller.

Både bestämmelsen i 3 kap. 1 § 1 mom. 16 punkten i lagförslag 1 och behandlingen av passageraruppgifter i lagförslag 2 måste stå i proportion till de särskilda säkerhetsmål som de syftar till att uppfylla. Avgränsningarna i direktivet föreslås genomföras helt, inklusive lagring och maskering av personuppgifter och begränsningar i användningen av dem, också med hänsyn

till de synpunkter som framkom i EU-domstolens yttrande i mål C-1/15 (Yttrande av Europeiska unionens domstol (stora avdelningen) 26.7.2017 – Europaparlamentet). Däremot föreslås det i lagförslag 2 att lagstiftningen ska utvidgas till att gälla också flygningar inom EU på det sätt som tillåts i direktivet. Det föreslås att de nationella bestämmelser som gäller andra transportörer ska bevaras i lagförslag 1 på det sätt som direktivet möjliggör, vilket dock innebär en avgränsning till enskilda fall på samma sätt som i den gällande lagen. Med beaktande av behoven att effektivt avvärja gränsöverskridande terroristbrott och annan grov brottslighet anses utvidgningarna nödvändiga för att uppnå målen med brottsbekämpningen.

I fråga om lagförslag 2 ska bestämmelserna om utlämnande av personuppgifter vara detaljerade. I synnerhet utlämnandet av personuppgifter från lufttrafikföretagen till polisen innebär att personuppgifter behandlas i stor skala och utlämnandet sker genom en teknisk anslutning. Dessutom får enheten för passagerarinformation lämna ut och överföra personuppgifter till andra behöriga myndigheter, enheter för passagerarinformation i EU:s medlemsstater, Europol och tredjeländer. Det föreslås inte någon reglering som går längre än den nivå som krävs i direktivet för utlämnandet av personuppgifter. Det anses därmed att utlämnandet av personuppgifter uppfyller det krav på proportionalitet som ställs i direktivet.

I lagförslag 2 föreslås det att den registrerades rätt till insyn i uppgifter om resultaten av behandlingen av passageraruppgifter (jämförelseuppgifter) ska begränsas. Däremot har den registrerade rätt till insyn i de personuppgifter som lufttrafikföretagen lämnat ut till polisen. Med beaktande av att det handlar om samma personuppgifter som lagrats i lufttrafikföretagens passagerarregister finns det inga skäl att begränsa rätten till insyn i fråga om de här uppgifterna. Till den del som det handlar om personuppgifter som lämnats ut till exempel för kriminalunderrättelseinhämtning bestäms begränsningen av rätten till insyn enligt bestämmelserna i lagförslag 1. Dataskyddsmyndigheten kan kontrollera om behandlingen av personuppgifterna är lagenlig med avseende på jämförelseuppgifterna. På så sätt begränsas den registrerades rätt till insyn inte mer än nödvändigt för att förebygga, avslöja eller utreda brott.

4.2 Jämlikhet

I 6 § i grundlagen finns en allmän klausul om jämlikhet och enligt den är alla lika inför lagen. Ingen får utan godtagbart skäl särbehandlas på grund av kön, ålder, ursprung, språk, religion, övertygelse, åsikt, hälsotillstånd eller handikapp eller av någon annan orsak som gäller hans eller hennes person. Den allmänna jämlikhetsklausulen kompletteras av förbudet mot diskriminering.

Den allmänna jämlikhetsklausulen riktas också till lagstiftaren. Vissa personer eller persongrupper får inte genom lag godtyckligt ges en gynnsammare eller ogynnsammare ställning än andra personer eller persongrupper. Enligt klausulen förutsätts det dock inte att alla människor ska bemötas lika i alla avseenden, om inte de förhållanden som inverkar är identiska. Grundlagsutskottet har i sin praxis ansett att den allmänna jämlikhetsprincipen inte kan sätta stränga gränser för lagstiftarens prövning när lagstiftningen ska anpassas efter samhällsutvecklingen vid en viss tidpunkt (GrUU 11/2012 rd, s. 2, GrUU 2/2011 rd, s. 2, GrUU 64/2010 rd, s. 2, GrUU 35/2010 rd, s. 2, GrUU 5/2008 rd, s. 4, GrUU 38/2006 rd, s. 2, GrUU 1/2006 rd, s. 2, GrUU 15/2001 rd, s. 2–3). Det viktigaste är om särbehandlingen kan motiveras på ett sätt som är godtagbart med hänsyn till systemet för de grundläggande fri- och rättigheterna (GrUU 46/2006 rd, s. 2, GrUU 16/2006 rd, s. 2, GrUU 73/2002 rd). Ur grundlagens likabehandlingsbestämmelser har utskottet i olika sammanhang härlett kravet att särbehandlingen inte får vara godtycklig och skillnaderna oskäliga (se exempelvis GrUU 11/2012 rd, s. 2, GrUU 37/2010 rd, s. 3, GrUB 11/2009 rd, s. 2, GrUU 18/2006 rd, s. 2). I 6 § 2 mom. i grundlagen finns en förteckning över ett antal förbjudna diskrimineringsgrunder. Förteckningen är dock inte uttömmande. Med de uttryckligen förbjudna diskrimineringsgrunderna jämställs "någon annan

orsak som gäller hans eller hennes person". Då grundlagsutskottet har tagit ställning till hurdan särbehandling som kan anses acceptabel har det också fäst avseende vid om den valda lösningen står i rätt proportion till det eftersträvade målet (GrUU 38/2006 rd, s. 3 och GrUU 23/2012 rd, s. 2). De åtgärder som gäller polisens behandling av personuppgifter får inte leda till diskriminerande behandling.

I 6 § 3 mom. i lagförslag 2 finns ett uttryckligt förbud enligt vilket de bedömningskriterier som tillämpas på jämförelsen av passageraruppgifter inte får grunda sig på uppgifter om en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, medlemskap i fackförbund, hälsotillstånd, sexualliv eller sexuella läggning. I lagförslag 2 har således förbudet mot diskriminering i enlighet med grundlagen beaktats. Genom bestämmelsen genomförs i lagförslag 2 samtidigt ett motsvarande förbud i dataskyddsdirektivet mot sådan etnisk profilering som kan leda till diskriminering.

I synnerhet skyldigheterna som gäller insamling av känsliga personuppgifter är viktiga att beakta vid bedömningen av om jämlikhetsprincipen följs. För att förebygga, avslöja och utreda brott kan polisen bli tvungen att på ett omfattande sätt behandla sådana känsliga personuppgifter som i värsta fall leder till diskriminering som strider mot grundlagen. Sådana uppgifter kan till exempel utgöras av uppgifter om brottsmisstänktas nationella eller etniska ursprung, eller deras hälsotillstånd, eller av genetiska uppgifter (DNA-spår) och fingeravtrycksuppgifter. Utöver den jämförelse av personuppgifter som avses i lagförslag 2 är särskilt den föreslagna utökade användningen av fingeravtryck som samlats in med stöd av 131 § i utlänningslagen betydelsefull med tanke på kravet på likabehandling i grundlagen. Förslaget avviker från möjligheten att dra nytta av fingeravtryck i pass i de fall som det handlar om grova brott.

Grundlagsutskottet har betonat behovet av att säkerställa att principen om ändamålsbundenhet följs i behandlingen av personuppgifter (se GrUU 33/2016 rd, s. 5, på finska, och de utlåtanden som det hänvisas till i det). Utskottet har i synnerhet i samband med bedömningen av de nationella bestämmelserna om behandlingen av biometriska identifieringsuppgifter betonat att när det gäller omfattande register med biometriska kännetecken finns det orsak att förhålla sig negativt till att uppgifterna används för ändamål som ligger utanför det syfte som de egentligen samlats in och registrerats för. Enligt grundlagsutskottet kan bara exakt avgränsade och obetydliga undantag göras från ändamålsbundenheten. Bestämmelserna får inte leda till att någon annan verksamhet än den som är förknippad med det ursprungliga ändamålet blir det huvudsakliga eller ens ett viktigt ändamål för registret (se till exempel GrUU 47/2010 rd, s. 3/II). Att fingeravtrycksuppgifter i passregistret får användas för att identifiera ett offer som annars inte kan identifieras kan enligt grundlagsutskottet ses som ett sådant exakt avgränsat och obetydligt undantag från ändamålsbundenheten som utskottet krävt (GrUU 47/2010 rd). Däremot har grundlagsutskottet betraktat en utvidgning av Eurodacsystemets ursprungliga användnings- och registreringsändamål till ändamål för laglighetskontroll som problematisk (se GrUU 14/2017 rd, GrUU 33/2016 rd, GrUU 21/2012 rd). Grundlagsutskottet har redan i ett tidigare utlåtande om ändring av utlänningslagen förutsatt att användningen av uppgifter om fingeravtryck som lagras nationellt i polisens register med stöd av 131 § i utlänningslagen ska begränsas uteslutande till ändamål som svarar mot det ändamål som de samlats in och registrerats för så att lagförslaget ska kunna behandlas i vanlig lagstiftningsordning. Grundlagsutskottet motiverade dock sitt utlåtande med att 16 § i lagen om behandling av personuppgifter i polisens verksamhet skulle ha tillämpats på användningen av fingeravtryck som registrerats utifrån den föreslagna lydelsen i 131 § i utlänningslagen, vilket hade gjort det möjligt att använda fingeravtrycksuppgifter för ändamål som på ett omfattande sätt och tydligt faller utanför det ändamål som de samlades in och registrerades för. Enligt utskottet var det helt klart att det inte handlade om sådana exakt avgränsade och obetydliga undantag från ändamålsbundenheten som utskottet krävt i sådana fall. Dessutom föreföll bestämmelserna ur grundlagsutskottets

synvinkel tvivelaktiga med beaktande av jämlikhetsbestämmelserna i 6 § i grundlagen i och med att de riktade sig mot vissa grupper av utlänningar (GrUU 47/2010 rd).

Med beaktande av grundlagsutskottets anmärkningar i ovannämnda utlåtande föreslås det inte att användningen av de fingeravtryck som tas av utlänningar med stöd av 131 § i utlänningslagen ska bindas till de allmänt tillämpliga bestämmelserna om förenlig behandling av personuppgifter som svarar mot kriterierna i 16 § i polisens gällande personuppgiftslag. Däremot finns det i lagförslag 1 en särskild bestämmelse i 2 kap. 11 § 5 mom. och i den avgränsas behandlingen av fingeravtryck närmare så att det handlar om ett obetydligt undantag från det ursprungliga ändamålet med behandlingen av dem. Undantaget innebär en inskränkning i uppfyllandet av jämlikhetsprincipen som garanteras i grundlagen utifrån medborgarskap. Med beaktande av proportionalitetsprincipen som gäller behandlingen av personuppgifter avgränsas undantaget enligt 2 kap. 11 § 5 mom. dock så att fingeravtrycksuppgifter som har samlats in för utförande av uppgifter enligt 131 § i utlänningslagen får användas för andra ändamål än de som uppgifterna ursprungligen har samlats in och registrerats för endast under samma förutsättningar som fingeravtryckuppgifter för pass samt när det är nödvändigt att använda uppgifterna för förebyggande, avslöjande eller utredning av sådana terroristbrott och andra grova brott som avses i Eurodacförordningen. Syftet med undantaget är att skydda den allmänna ordningen och säkerheten, som när det gäller grova brott har ett nära samband med upprätthållandet av statens säkerhet. Den föreslagna utvidgningen anses nödvändig för att skydda den nationella säkerheten och den allmänna säkerheten och den bedöms vara proportionell i förhållande till det tungt vägande samhälleliga intresse som ska skyddas. Rätt att använda uppgifterna har endast den som nödvändigtvis behöver dem för skötseln av sina arbetsuppgifter. Undantaget är därmed noggrant avgränsat på det sätt som grundlagens tolkningspraxis kräver.

Polisen har med stöd av 131 § i utlänningslagen rätt att ta signalement för tryggande av statens säkerhet. Enligt Europakonventionens tolkningspraxis har staten bred prövningsmarginal i fråga om vilka åtgärder som är nödvändiga för att trygga statens säkerhet. För tryggandet av säkerheten anses det viktigt bland annat att utreda vem det finns skäl att misstänka för genomförande eller planering av brott som äventyrar statens säkerhet. Behandlingen av biometriska fingeravtrycksuppgifter avgränsas till att gälla situationer när det är nödvändigt för att identifiera en person. Enligt lagförslag 1 ska förebyggande, avslöjande och utredning av terroristbrott och andra grova brott betraktas som ett med tryggande av statens säkerhet förenligt ändamål med behandlingen av personuppgifter. Till det tryggande av statens säkerhet som avses i 131 § i utlänningslagen hör dels polisens lagstadgade uppgift om övervakning av utlänningar, dels skyddspolisens uppgift att upprätthålla den nationella säkerheten. Enligt 34 a kap. 1 § 1 mom. i strafflagen är en gärning i terroristiskt syfte ägnad att allvarligt skada en stat. Det föreslås att andra grova brott ska jämställas med terroristhandlingar och de kan utgöras av sådana brott som avses i bestämmelsen i fråga i strafflagen då det terroristiska syftet fattas. I Europadomstolens rättspraxis har staten ansetts ha en bred prövningsmarginal bland annat vid bedömningen av om inskränkningen av integritetsskyddet är nödvändig för att trygga statens säkerhet (Leander mot Sverige, 26.3.1987, punkt 59 i domen). Den kontroll som framkommit i Europadomstolens rättspraxis hör dock samman med prövningsmarginalen. Europadomstolen har dock förhållit sig försiktigt till en begränsning av den grundläggande rättighet som gäller likabehandling. Enligt domstolens tolkningspraxis ska det finnas tungt vägande skäl för att begränsa rättigheterna i artikel 14 utifrån medborgarskap trots statens prövningsmarginal (Andrejeva mot Lettland, 18.2.2009, punkterna 88–91 i domen). Den föreslagna begränsningen av skyddet för privatlivet, som samtidigt ingriper i jämlikhetsprincipen, bedöms i enlighet med lagförslag 1 vara nödvändig i ett demokratiskt samhälle för att uppnå målen om förebyggande, avslöjande och utredning av brott samt upprätthållande av statens säkerhet. Begränsningen bedöms inte gå längre än vad som är nödvändigt för att identifiera personer med koppling till brottslig verksamhet.

Enligt grundlagsutskottet kan ett ändamål som motsvarar fingeravtryckens ursprungliga behandlingsändamål i sig ha samband med att förhindra och utreda exakt angivna brott, men bara i den omfattning som verksamheten har ett nära samband med det ursprungliga insamlings- och registreringsändamålet (GrUU 47/2010 rd). Med hänsyn till att ett av de ursprungliga ändamålen med att registrera signalement enligt 131 § i utlänningslagen är att trygga statens säkerhet och att terroristbrott och andra grova brott till sin karaktär är brott som äventyrar den allmänna ordningen och säkerheten och statens säkerhet, har den föreslagna begränsningen ett nära samband med det ursprungliga ändamålet med behandlingen av personuppgifterna. Den föreslagna bestämmelsen är också avgränsad till att gälla förebyggande, avslöjande och utredning av de här brotten och de föreslagna åtgärderna som begränsar skyddet för privatlivet går inte längre än vad som är nödvändigt. Fingeravtryck är ofta det enda tillförlitliga sättet att identifiera en person, i synnerhet någon som inte är finländsk medborgare, varför begränsningen anses nödvändig också med tanke på jämlikhetsprincipen. Vid tillämpningen av den föreslagna bestämmelsen ska man dock beakta att den inte får leda till diskriminering. Fingeravtryck används endast i den mån som det är nödvändigt för att identifiera en person. Lagförslag 1 kan till denna del anses uppfylla kraven i grundlagen.

4.3 Administrativa påföljder och ändringssökande

Skyddet för de grundläggande fri- och rättigheterna gäller i regel fysiska personer. De grundläggande fri- och rättigheterna kan dock skydda en juridisk person indirekt, när avsaknaden av en ställning som juridisk person kan innebära att man gör intrång i rättigheter som tillkommer en individ bakom den juridiska personen (RP 309/1993 rd, s. 21–25). Med tanke på juridiska personers ställning är lagförslag 2 i propositionen betydelsefullt, i synnerhet till de delar som gäller påföljderna vid försummelse av en lagstadgad skyldighet i samband med lufttrafikföretagens verksamhet och möjligheten att söka ändring i en myndighets förvaltningsbeslut. En enskild person kan också stå bakom försummelsen, även om påföljden påförs den juridiska personen. I lagförslag 2 har lufttrafikföretagen ålagts en skyldighet att till enheten för passagerarinformation avgiftsfritt överföra passageraruppgifter för de ankommande och avgående flygningar utanför eller inom Europeiska unionen som de utför, till den del uppgifterna har samlats in som en del av den normala affärsverksamheten samt eventuell förhandsinformation om passagerare om sådan samlats in. I lagen föreskrivs det också om på vilket sätt de här uppgifterna i regel ska överföras. Uppgifterna ska överföras elektroniskt och det förutsätts att lufttrafikföretagen ska använda en särskild teknisk anslutning och överföra uppgifterna systematiskt för varje flygning över EU:s gränser. Hittills har lufttrafikföretagen överfört passageraruppgifter till polisen endast på basis av en enskild begäran. Lufttrafikföretag som bryter mot den föreskrivna skyldigheten att överföra passageraruppgifter ska kunna påföras en påföljdsavgift (påföljdsavgift för lufttrafikföretag). Påföljdsavgiften ska kunna påföras för varje sådan flygning för vilken passageraruppgifter inte har överförts eller för vilken uppenbart bristfälliga uppgifter överförts.

Enligt grundlagsutskottets vedertagna tolkningspraxis är en påföljdsavgift som påförs för en lagstridig gärning inte en skatt eller avgift enligt grundlagens 81 § utan en ekonomisk påföljd av straffnatur. I sak har utskottet jämställt en penningmässig påföljd av straffnatur med en straffrättslig påföljd (GrUU 4/2001 rd, s. 7, GrUU 32/2005 rd, s. 2, GrUU 55/2005 rd, s. 2, GrUU 17/2012 rd s. 5). De allmänna grunderna för en administrativ påföljd måste enligt 2 § 3 mom. i grundlagen föreskrivas genom lag, eftersom påförandet av den inbegriper utövande av offentlig makt. Enligt grundlagsutskottet måste det i lagen finnas klara och specifika bestämmelser om grunderna för påföljden och dess belopp och om rättsskyddet liksom om grunderna för lagens verkställighet (GrUU 32/2005 rd, s. 2–3, GrUU 55/2005 rd, s. 2, GrUU 57/2010 rd, s. 2, GrUU 17/2012 rd s. 5). Grundlagsutskottet har konstaterat att även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen i grundlagens 8 § inte direkt gäller bestämmelser om administrativa påföljder kan det allmänna kravet på exakthet ändå inte förbigås i ett sam-

manhang som här (GrUU 9/2012 rd, s. 2, GrUU 57/2010 rd, s. 2 och GrUU 74/2002 rd, s. 5). I lagförslag 2 föreskrivs det detaljerat om de grunder enligt vilka påföljdsavgift får påföras, dess belopp samt om verkställigheten av påföljdsavgiften och ändringssökande.

Bestämmelser om påföljder ska enligt grundlagsutskottets tolkningspraxis också vara proportionerliga (GrUU 58/2010 rd, s. 5, GrUU 11/2009 rd, s. 7-8, GrUU 12/2006 rd, s. 3, GrUU 74/2002 rd, s. 5). Proportionaliteten är förenad med frågan om påföljder vid ringa försummelser (GrUU 58/2010 rd, s. 6, GrUU 12/2006 rd, s. 2–3). I PNR-direktivet förutsätts att påföljderna ska vara effektiva, proportionella och avskräckande. I lagförslag 2 föreslås att polisen ska få rätt att påföra en påföljdsavgift vars maximilopp uppgår till 3 000 euro per flygning. I den föreslagna bestämmelsen är det inte fråga om en påföljd som är betydande till sitt belopp, fastän den påförs för varje sådan flygning för vilken passageraruppgifter inte har överförts. Påföljdsavgift för lufttrafikföretag påförs inte om det vid överföringen av passageraruppgifterna har inträffat ett fel till följd av ouppmärksamhet som med beaktande av samtliga omständigheter är ursäktlig eller om det i övrigt med hänsyn till omständigheterna skulle vara oskäligt att påföra en avgift. Påföljdsavgift får inte heller påföras den som är misstänkt för samma gärning i en förundersökning eller åtalsprövning eller i ett brottmål som är anhängigt vid en domstol eller den som genom en lagakraftvunnen dom har dömts till straff för samma gärning eller som för brott mot 20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) har påförts påföljdsavgift för transportör enligt 179 § i utlänningslagen (301/2004). Den föreslagna påföljdsavgiften kan således anses vara proportionerlig på det sätt som grundlagsutskottet förutsätter.

Det måste gå att söka ändring i ett beslut om påförande av en administrativ påföljd. Möjligheten att söka ändring i en myndighets beslut kan vara behövlig för att säkerställa att myndigheterna beter sig på ett behörigt och i övrigt opartiskt sätt (GrUU 32/2012 rd, s. 4–5, GrUU10/2009 rd, s. 4, GrUU 55/2002 rd, s. 4, GrUU 47/2002 rd, s. 4, GrUU 46/2002 rd, s. 9) liksom för att säkerställa en enhetlig tillämpningspraxis (GrUU 30/2005 rd, s. 5, GrUU13/2005 rd, s. 3–4, GrUU 33/2000 rd, s. 3), även om det inte handlar om ett ärende som gäller individens rättigheter eller skyldigheter. När föremålet för sökandet av ändring är ett beslut om påförande av en administrativ påföljd som grundar sig på utövning av offentlig makt, ska ändringssökandet i regel ordnas i enlighet med förvaltningsprocesslagen (586/1996) (GrUU 4/2005 rd, s. 3/II). Vid bedömningen av om rättsskyddet är ändamålsenligt har man också beaktat om en administrativ påföljd kan verkställas oberoende av besvär (GrUU 4/2004 rd, s. 7). Enligt 21 § i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring samt andra garantier för en rättvis rättegång och god förvaltning ska tryggas genom lag.

Lufttrafikföretaget har rätt att bli hört innan påföljdsavgiften för transportör påförs. I lagen föreskrivs också om ändringssökande. En påföljdsavgift som påförts med stöd av lagen verkställs i den ordning som föreskrivs i lagen om verkställighet av böter. Ett beslut om påföljdsavgift för lufttrafikföretag får överklagas genom besvär hos förvaltningsdomstolen på det sätt som föreskrivs i förvaltningsprocesslagen (586/1996). Förvaltningsdomstolens beslut får överklagas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Med beaktande av de rättsskyddsgarantier som det föreskrivs om för lufttrafikföretag ska förslaget inte betraktas som problematiskt med tanke på rättsskyddet i enlighet med grundlagen.

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

1.

Lag

om behandling av personuppgifter i polisens verksamhet

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om helt eller delvis automatiserad behandling av personuppgifter som behövs för skötseln av polisens uppgifter enligt 1 kap. 1 § i polislagen (872/2011) samt om annan behandling av personuppgifter, då personuppgifterna utgör eller är avsedda att utgöra ett personregister eller en del av ett sådant.

2 §

Förhållande till annan lagstiftning

På behandlingen av personuppgifter i syfte att förebygga, avslöja eller utreda brott eller föra brott till åtalsprövning, inklusive att skydda mot eller förebygga hot mot den allmänna säkerheten, tillämpas lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/), om inte något annat föreskrivs i denna lag.

På annan behandling av personuppgifter tillämpas Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, nedan *dataskyddsförordningen*, samt dataskyddslagen (/), om inte något annat föreskrivs i denna lag.

Bestämmelser om nödcentralsdatasystemet finns i lagen om nödcentralsverksamhet (692/2010) och om utlänningsregistret i lagen om utlänningsregistret (1270/1997).

På sekretess och tystnadsplikt i fråga om personuppgifter tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999).

3 §

Definitioner

Utöver vad som föreskrivs om definitioner i 3 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och i artikel 4 i dataskyddsförordningen, avses i denna lag med

1) *författningsgrunden för Schengens informationssystem* Europaparlamentets och rådets förordning (EG) nr 1987/2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II), rådets beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) samt Europaparlamentets och rådets förordning (EG) nr 1986/2006 om tillträde till andra generationen av

Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon,

2) *Schengens informationssystem* andra generationen av Schengens informationssystem så som det definieras i författningsgrunden för Schengens informationssystem (SIS II),

3) *det nationella systemet inom Schengens informationssystem* systemet N.SIS II enligt författningsgrunden för Schengens informationssystem,

4) *Schengenstat* en stat som använder Schengens informationssystem,

5) *behöriga Schengenmyndigheter* polisen, gränsbevakningsväsendet, Tullen, försvarsmakten, åklagarna, Migrationsverket, Trafiksäkerhetsverket, utrikesministeriet samt finländska beskickningar, om utrikesministeriet har beviljat en finsk medborgare som tjänstgör där behövligt bemyndigande att bevilja visum,

6) *Sirenekontoret* centralkriminalpolisen,

7) *Europolförordningen* Europaparlamentets och rådets förordning (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF,

8) *Europols nationella enhet* centralkriminalpolisen, som är det sambandsorgan mellan Europol och de behöriga myndigheterna i medlemsstaten som avses i Europolförordningen,

9) *Eurodacförordningen* Europaparlamentets och rådets förordning (EU) nr 603/2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa.

2 kap.

Behandling av personuppgifter

1 §

Behandling av grundläggande personuppgifter

Polisen får för de ändamål som anges i 3–5 och 9 § behandla följande behövliga grundläggande personuppgifter:

1) personens namn,
2) födelsedatum och födelseort,
3) personbeteckning,
4) kön,
5) modersmål,
6) kontaktspråk,
7) civilstånd,
8) medborgarskap eller avsaknad av medborgarskap samt nationalitet,
9) hemvist och bostadsort,
10) yrke och utbildning,
11) kontaktuppgifter,
12) uppgifter ur handlingar som behövs för att fastställa identiteten,
13) i fråga om en utländsk person föräldrarnas namn, medborgarskap och nationalitet,
14) uppgifterna i ett resedokument samt övrig behövlig information som gäller inresa och passerande av gräns,
15) klientnummer som en myndighet gett,

16) uppgift om att personen avlidit eller om dödförklaring av personen, och
17) övriga nödvändiga uppgifter som kan jämställas med de uppgifter som nämns ovan.

Utöver de grundläggande personuppgifter som avses i 1 mom. får polisen behandla behövliga uppgifter om intressebevakning, försättande i konkurs och meddelande om näringsförbud samt fullgörande av värnplikt.

2 §

Behandling av andra personuppgifter som anknyter till det behandlade ärendet

Polisen får utöver de grundläggande personuppgifter som avses i 1 § dessutom behandla andra behövliga personuppgifter som ingår i det behandlade ärendet eller i polisens uppgifter, åtgärder eller händelser. Personuppgifterna ska anknyta till ett sådant ändamål med behandlingen som föreskrivs i 3–5 eller 9 §.

I anknytning till behandlingen av sådana ärenden, uppgifter, åtgärder eller händelser som avses i 1 mom. får polisen också behandla särskilda kategorier av personuppgifter som är nödvändiga för skötseln av de uppgifter som avses i 3–5 §, signalement som avses i tvångsmedelslagen samt särskilda kategorier av personuppgifter som behövs för skötseln av de uppgifter som avses i 9 §. För att personer som anmälts försvunna ska kunna hittas och för att okända avlidna ska kunna identifieras får nödvändiga biometriska och genetiska uppgifter om nära släktingar registreras endast med samtycke av den som uppgifterna gäller.

För skötseln av de uppgifter som föreskrivs för polisen i 131 § i utlänningslagen (301/2004) får polisen behandla de i den paragrafen avsedda signalementen (*uppgifter för identifiering av utlänningar*).

För de ändamål som anges i 3 och 4 § får polisen behandla uppgifter om en i 5 kap. 40 § i polislagen eller 10 kap. 39 § i tvångsmedelslagen avsedd person som har använts som informationskälla, uppgifter om hur informationskällan har använts och om tillsynen samt det huvudsakliga innehållet i de uppgifter som informationskällan lämnat (*uppgifter om informationskälla*).

För att trygga säkerheten för en person som är föremål för en åtgärd eller en myndighets säkerhet i arbetet får polisen behandla nödvändiga uppgifter om en persons hälsotillstånd och hur hälsotillståndet följs eller om vårdåtgärder, uppgifter om hur farlig eller oberäknelig ett objekt eller en person är samt uppgifter som beskriver eller är avsedda att beskriva en brottslig gärning, ett straff eller någon annan påföljd för brott (*säkerhetsinformation*).

3 §

Behandling av personuppgifter i utredningssyfte

Polisen får behandla personuppgifter som anknyter till förundersökning, polisundersökning, andra åtgärder i anknytning till förebyggande, utredning eller avslöjande av brott eller användning av tvångsmedel.

De i 1 mom. avsedda uppgifterna ska anknyta till någon av följande personer:
1) den som är misstänkt för ett brott eller medverkar i ett brott,
2) en person som inte har fyllt 15 år och är misstänkt för en brottslig gärning,
3) den som är föremål för förundersökning, polisundersökning eller polisens åtgärder,
4) den som har anmält ett brott eller uppträder som målsägande,
5) ett vittne,
6) ett offer,
7) den som har använts som informationskälla, eller
8) den som har något annat samband med ärendet.

De i 2 mom. avsedda personuppgifterna, som rör olika kategorier av registrerade, ska så långt det är möjligt åtskiljas från varandra.

4 §

Behandling av personuppgifter som anknyter till kriminalunderrättelseinhämtning

Polisen får behandla personuppgifter som anknyter till kriminalunderrättelseinhämtning

1) för sådan kriminalunderrättelseinhämtning och brottsanalys, samt för att utföra uppgifter i anknytning till dessa, som behövs för att förebygga, avslöja eller utreda brott på vilka det kan följa fängelse,

2) för att utarbeta sådana strategiska och tematiska analyser som behövs för att utföra en uppgift.

De i 1 mom. avsedda uppgifterna ska anknyta till personer som

1) kan antas ha gjort sig eller göra sig skyldiga till brott,

2) kan antas ha främjat eller främja brott på vilket det kan följa fängelse i mer än sex månader, eller straffbart bruk av narkotika, eller

3) upprepat har kontakt med en i 1 eller 2 punkten avsedd person eller upprepat påträffas i dennes sällskap, och kontakten eller sammanträffandena antas ha samband med ett brott,

4) är föremål för observation i enlighet med 5 kap. 13 § 1 mom. i polislagen eller 10 kap. 12 § i tvångsmedelslagen.

Polisen får när det är nödvändigt för att förebygga, avslöja eller utreda ett brott behandla i 1 mom. avsedda uppgifter också i fråga om följande kända personer:

1) vittnen till ett brott,

2) offer för ett brott,

3) den som har anmält ett brott eller uppträder som målsägande.

Till personuppgifter som anknyter till kriminalunderrättelseinhämtning ska det om möjligt fogas en bedömning av uppgiftslämnarens eller källans tillförlitlighet och uppgifternas riktighet.

5 §

Behandling av personuppgifter för upprätthållande av allmän ordning och säkerhet

Polisen får behandla personuppgifter för att utföra uppdrag i anknytning till att trygga rätts- och samhällsordningen eller upprätthålla allmän ordning och säkerhet, för att utföra för polisen föreskrivna övervakningsuppdrag eller handräckningsuppdrag, för att utföra polisundersökning enligt 6 kap. i polislagen eller för att upprätthålla ordningen och säkerheten i en förvaringslokal.

6 §

Behandling av observationsuppgifter

Polisen har rätt att registrera uppgifter om observationer som gjorts av polismän eller uppgifter som anmälts till polisen i anslutning till händelser eller personer som utifrån omständigheterna eller en persons hotelser eller uppträdande i övrigt med fog kan bedömas ha samband med brottslig verksamhet (*observationsuppgifter*). Till observationsuppgifterna ska det om möjligt fogas en bedömning av uppgiftslämnarens eller källans tillförlitlighet och uppgifternas riktighet.

7 §

Behandling av uppgifter som inte hänför sig till ett visst uppdrag

Personuppgifter som fåtts i samband med polisuppdrag och som behövs för att de uppgifter som föreskrivs i 1 kap. 1 § i polislagen ska kunna utföras, men som inte hänför sig till ett pågående uppdrag, får behandlas för de ändamål och enligt de villkor som föreskrivs i 3–6 §.

Polisen får på beslut av en polisman som hör till befälet behandla personuppgifter som fåtts i samband med uppdrag och som kan vara av betydelse för utförandet av sådana uppdrag som föreskrivs i 1 kap. 1 § i polislagen, för att klarlägga om uppgifterna behövs för sådana ändamål med behandlingen som föreskrivs i 3–6 §. Onödiga uppgifter ska utplånas utan dröjsmål.

8 §

Behandling av överskottsinformation som erhållits med hemliga informationsinhämtningsmetoder

Överskottsinformation som fåtts med sådana hemliga informationsinhämtningsmetoder som avses i 5 kap. i polislagen samt överskottsinformation som inhämtats med sådana hemliga tvångsmedel som avses i 10 kap. i tvångsmedelslagen får registreras för sådana ändamål med behandlingen av personuppgifter som föreskrivs i 3 och 4 §.

Bestämmelser om användning av överskottsinformation finns i 5 kap. 54 § i polislagen och bestämmelser om användning av överskottsinformation som fåtts genom hemliga tvångsmedel finns i 10 kap. 56 § i tvångsmedelslagen.

9 §

Behandling av personuppgifter i tillståndsförvaltnings- och tillsynsuppgifter samt i uppgifter enligt hittegodslagen

Polisen får behandla personuppgifter för att utföra de uppgifter som föreskrivs i hittegodslagen (778/1988), skjutvapenlagen (1/1998), lagen om skjutbanor (763/2015), lagen om identitetskort (663/2016), passlagen (671/2006), lagen om privata säkerhetstjänster (1085/2015), lagen om saluföring och användning av sprängämnesprekursorer (653/2014), lagen om penninginsamlingar (255/2006), lotterilagen (1047/2001) och lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017).

De personuppgifter som behandlas för att utföra de uppgifter som avses i 1 mom. ska anknyta till personer som

1) är nuvarande eller tidigare tillståndssökande eller tillståndshavare samt anmälare,

2) är kontakt- eller ansvarspersoner inom sammanslutningar som ansöker om tillstånd eller är tillståndshavare, andra företrädare för sammanslutningarna eller personer som med stöd av skjutvapenlagen registrerats som anmälda till eller deltagare i ett prov för ansvarig person,

3) en skjutvapenanmälan i enlighet med 114 § i skjutvapenlagen gäller,

4) är kontakt- eller ansvarspersoner för penninginsamlingar eller lotterier eller genomför sådana i praktiken,

5) är anställda hos ett penningspelsbolag eller en annan näringsidkare eller sammanslutning som i enlighet med bestämmelserna i lotterilagen eller lagen om förhindrande av penningtvätt och av finansiering av terrorism ska övervakas av polisen,

6) är rapportörer eller föremål för rapporter i enlighet med 7 kap. 9 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism,

7) har något annat samband med de uppgifter som avses i 1 mom.

Polisen får som en del av tillsynen i enlighet med lotterilagen och lagen om förhindrande av penningtvätt och av finansiering av terrorism i den utsträckning som det är nödvändigt för att polisens tillsynsuppgift ska kunna utföras behandla personuppgifter för kunderna hos ett penningspelsbolag eller en annan näringsidkare eller sammanslutning som polisen enligt de nämnda lagarna ska övervaka.

10 §

Behandling av personuppgifter som fåtts vid teknisk övervakning

Polisen har rätt att behandla personuppgifter som har fåtts vid sådan teknisk övervakning som avses i 4 kap. 1 § i polislagen.

11 §

Förenlig behandling

Om inte något annat föreskrivs i denna eller någon annanstans i lag, får polisen behandla personuppgifter för andra ändamål än det ursprungliga ändamålet med insamlingen och registreringen av uppgifterna, med undantag för sådana uppgifter om tillsyn i fråga om penningspelsbolag som avses i lotterilagen och i lagen om förhindrande av penningtvätt och av finansiering av terrorism, när detta behövs för

1) att förebygga, avslöja eller utreda ett brott på vilket kan följa fängelse,
2) att påträffa en efterlyst,
3) en utredning som stöder det att någon är oskyldig,
4) att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada,
5) att trygga den nationella säkerheten,
6) utredning av identitet i samband med ett visst polisuppdrag som nödvändigt kräver att identiteten styrks,
7) att fatta beslut eller lämna utlåtande om beviljande av ett tillstånd eller tillståndets giltighet, när tillståndet enligt gällande bestämmelser är beroende av sökandens eller tillståndshavarens tillförlitlighet, lämplighet eller någon liknande egenskap, och det för bedömningen av egenskapen krävs uppgifter om sökandens eller tillståndshavarens hälsotillstånd, bruk av berusningsmedel, brottslighet eller våldsamma uppträdande.

Utöver vad som föreskrivs i 5 § 3 mom. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten får uppgifter i polisens personregister trots sekretessbestämmelserna behandlas även för laglighetsövervakning och för analys- planerings- och utvecklingsverksamhet. Uppgifter får också användas för utbildningsverksamhet, om de är nödvändiga för att genomföra utbildningen.

De observationsuppgifter som avses i 6 §, uppgifter som insamlats och registrerats i kriminalunderrättelsesyfte enligt 4 § eller för det ändamål som avses i 7 § 2 mom. får inte användas för utförandet av de uppgifter som avses i 1 mom. 7 punkten.

Fingeravtrycksuppgifter som för utförande av de uppgifter som föreskrivs i passlagen har samlats in om den som ansöker om pass får användas för andra ändamål än det ursprungliga ändamålet med behandlingen av uppgifterna endast om det är nödvändigt för att identifiera ett offer för en naturkatastrof, storolycka eller någon annan katastrof eller ett brott eller ett offer som annars förblivit oidentifierat. Rätt att använda uppgifterna har endast den som nödvändigtvis behöver dem för skötseln av sina arbetsuppgifter. Uppgifter som tagits för jämförelse får användas endast när jämförelsen görs och ska därefter förstöras omedelbart.

Fingeravtrycksuppgifter som har samlats in för utförande av uppgifter enligt 131 § i utlänningslagen får användas för andra ändamål än de som uppgifterna ursprungligen har samlats in och registrerats för endast i de fall som avses i 4 mom. samt när det är nödvändigt att an-

vända uppgifterna för förebyggande, avslöjande eller utredning av sådana terroristbrott och andra grova brott som avses i Eurodacförordningen. Rätt att använda uppgifterna har endast den som nödvändigtvis behöver dem för skötseln av sina arbetsuppgifter.

Uppgifter i en skjutvapenanmälan enligt 114 § i skjutvapenlagen får inte användas för andra ändamål än för behandling av uppgifter som gäller vapentillstånd.

3 kap.

Särskilda bestämmelser om behandling av personuppgifter

1 §

Polisens rätt att få uppgifter ur vissa register och informationssystem

Utöver vad som föreskrivs i någon annan lag har polisen trots sekretessbestämmelserna rätt att i enlighet med vad som avtalas om saken med den personuppgiftsansvarige i fråga ur vissa register genom en teknisk anslutning eller som en datamängd få sådan information som polisen behöver för att utföra sina uppdrag och föra sina personregister, enligt följande:

1) ur det fordonstrafikregister som avses i lagen om fordonstrafikregistret (541/2003) för uppdrag som avses i 15–17 § i den lagen,

2) uppgifter som gäller dömda, fångar eller intagna i en enhet vid Brottspåföljdsmyndigheten ur Brottspåföljdsmyndighetens informationssystem på det sätt som anges i 14 § 1 och 2 mom. i lagen om behandling av personuppgifter vid Brottspåföljdmyndigheten (1069/2015) för förhindrande, utredning och överlämnande för åtalsprövning av brott eller för ett sådant tillstånd eller godkännande från polisen som förutsätter att personen i fråga är tillförlitlig,

3) ur kommunikationsministeriets trafiktillståndsregister de uppgifter som behövs för trafikövervakning, förundersökning, annan undersökning och för påförande av påföljdsavgift för tranportör enligt 179 § i utlänningslagen,

4) av dem som utövar inkvarteringsverksamhet sådana uppgifter om resande som avses i 6 § 1 mom. i lagen om inkvarterings- och förplägnadsverksamhet (308/2006) och som behövs för att upprätthålla allmän ordning och säkerhet samt för att förhindra, avslöja eller utreda brott och för att utföra något annat för polisen lagstadgat uppdrag,

5) ur det bötesregister som avses i lagen om verkställighet av böter (672/2002), för de ändamål som nämns i 50 § i den lagen, uppgifter om brott och straffrättsliga påföljder samt för behandling av tillståndsärenden, ur det straffregister som avses i straffregisterlagen (770/1993), för de ändamål som nämns i 4 och 4 a § i den lagen, personuppgifter och av justitieförvaltningsmyndigheterna uppgifter om personer som är efterlysta av dem, ur det register över avgöranden och meddelanden om avgöranden som avses i lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) uppgifter om avgöranden i brottmål och om avgörandenas laga kraft samt ur det rikssystem för behandling av diarie- och ärendehanteringsuppgifter som avses i den lagen uppgifter om brottmål som är eller har varit anhängiga vid åklagarmyndigheter eller domstolar, om sådan information kan fås,

6) ur Patent- och registerstyrelsens handelsregister, för förhindrande, avslöjande och utredande av brott, uppgifter om anmälningar och meddelanden som gäller näringsidkare,

7) ur gränsbevakningsväsendets och Tullens personregister, för polisuppdrag som motsvarar de uppdrag för vilka uppgifterna har samlats in och registrerats för samt för andra ändamål när det gäller fall som avses i 16 § 1 mom.,

8) ur utrikesministeriets informationssystem, för förundersökning, annan undersökning och för utförande av de uppdrag som föreskrivs för polisen i utlänningslagen, uppgifter om dem som hör till personalen vid diplomatiska beskickningar och konsulat som representerar den utsändande staten i Finland och om dem som hör till personalen vid en internationell organisations organ i Finland eller något annat internationellt organ i samma ställning samt om dessa personers familjemedlemmar och om dem som är i privat tjänst hos dessa personer,

9) ur Migrationsverkets informationssystem, för förundersökning, annan undersökning och för utförande av de uppdrag som föreskrivs för polisen i utlänningslagen, uppgifter om ärenden som gäller resedokument, visum, vistelse, internationellt skydd, avlägsnande ur landet, inreseförbud och medborgarskap,

10) ur det farkostregister som avses i lagen om farkostregistret (424/2014) och ur Ålands fritidsbåtsregister sådana uppgifter om båtar och ägare och innehavare av båtar som behövs för utförande av de uppgifter som anges i 1 kap. 1 § i polislagen och de uppdrag som avses i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) samt för påförande av påföljdsavgift för transportör enligt 179 § i utlänningslagen,

11) av ett teleföretag de uppgifter som avses i 10 kap. 6–8 § i tvångsmedelslagen, i 5 kap. 8 och 9 § i polislagen samt i 19 kap. i informationssamhällsbalken (917/2014),

12) av den myndighet som har begärt handräckning, uppgifter som behövs för lämnande av handräckning,

13) de uppgifter som anges i 13–17 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009),

14) ur försvarsmaktens värnpliktsregister, för bedömningen av den personliga lämpligheten hos en person som söker eller innehar ett tillstånd som avses i skjutvapenlagen och en person för vilken ett godkännande som avses i skjutvapenlagen söks eller som har fått ett sådant godkännande, i 97 a § i värnpliktslagen (1438/2007) avsedda nödvändiga uppgifter om en värnpliktigs tjänstgöring och tjänsteduglighet,

15) ur det register över kompetensbrev för laddare som avses i 22 § i lagen om laddare (423/2016) uppgifter för övervaknings- och larmuppdrag samt för förhindrande, utredning och avslöjande av brott,

16) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för att förhindra, avslöja och utreda brott och föra brott till åtalsprövning samt för att nå efterlysta personer; bestämmelser om rätten att få uppgifter ur flygtrafikens passageraruppgiftssamlingar finns i lagen om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (/).

Polisen har rätt att få de uppgifter som avses i 1 mom. avgiftsfritt, om inte något annat föreskrivs i lag.

Polisen ska på begäran ge den personuppgiftsansvarige information om behandlingen av de uppgifter som polisen fått med stöd av 1 mom. Om personuppgifter har lämnats ut utan begäran, ska polisen utan dröjsmål granska om uppgifterna behövs för det ändamål för vilket de har lämnats ut.

2 §

Uppgifter som andra myndigheter lämnar ut till polisen genom registrering vid direkt anslutning eller för registrering som en datamängd

Enligt avtal med den personuppgiftsansvarige kan uppgifter lämnas till polisens personregister genom direkt anslutning eller för registrering som en datamängd enligt följande:

1) av justitieförvaltningsmyndigheterna, Brottspåföljdsmyndigheten och Rättsregistercentralen uppgifter om personer som de har efterlyst, av Brottspåföljdsmyndigheten signalementsuppgifter om personer som avtjänar eller har avtjänat straff som riktar sig mot friheten och av Rättsregistercentralen uppgifter om besöksförbud och näringsförbud,

2) av Tullen och militärmyndigheterna uppgifter om personer som de har efterlyst och av Tullen uppgifter om identifiering av utlänningar och uppgifter som behövs för förebyggande och utredning av brott,

3) av utrikesministeriet och finska beskickningar uppgifter som behövs för skötseln av utrikesministeriets och finska beskickningars uppdrag enligt passlagen, av utrikesministeriet uppgifter om dem som hör till personalen vid diplomatiska beskickningar och konsulat som repre-

senterar den utsändande staten i Finland och om dem som hör till personalen vid en internationell organisations organ i Finland eller något annat internationellt organ i samma ställning samt om dessa personers familjemedlemmar och om dem som är i privat tjänst hos dessa personer,

4) av gränsbevakningsväsendet i 2 § avsedda uppgifter som ska behandlas för utförande av de uppdrag enligt 1 kap. 1 § 1 mom. i polislagen som föreskrivs för gränsbevakningsväsendet i gränsbevakningslagen (578/2005) eller någon annanstans i lag, samt i 3 § i denna lag avsedda uppgifter som ska behandlas för utförande av de uppdrag enligt 1 kap. 1 § 2 mom. i polislagen som föreskrivs för gränsbevakningsväsendet i gränsbevakningslagen eller någon annanstans i lag,

5) av Forststyrelsens jakt- och fiskeövervakare sådana behövliga uppgifter om vidtagna åtgärder som registrerats vid jakt- och fiskeövervakning som hör till deras behörighet,

6) av nödcentralsmyndigheterna uppgifter om en person som har registrerats i nödcentralsdatasystemet när uppgifterna behövs med tanke på den registrerades egen säkerhet eller säkerheten i arbetet,

7) av Migrationsverket uppgifter om nationella inreseförbud samt om polisåtgärder i anslutning till beslut om avvisning och utvisning och handräckning.

Polisen ska på begäran ge den personuppgiftsansvarige information om behandlingen av de uppgifter som polisen fått med stöd av 1 mom. Om personuppgifter har lämnats ut utan begäran, ska polisen utan dröjsmål granska om uppgifterna behövs för det ändamål för vilket de har lämnats ut.

3 §

Europeiska unionens informationssystem för viseringar

Polisen har rätt att genom teknisk anslutning få uppgifter ur Europeiska unionens informationssystem för viseringar (VIS) för utförande av en uppgift som enligt utlänningslagen ska skötas av polisen i enlighet med bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 767/2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen).

Dessutom har polisen rätt att genom teknisk anslutning få uppgifter ur Europeiska unionens informationssystem för viseringar i syfte att förhindra och utreda terroristbrott som avses i 34 a kap. i strafflagen och brott som avses i 3 § 2 mom. i lagen om utlämning för brott mellan Finland och de övriga medlemsstaterna i Europeiska unionen (1286/2003), på det sätt som anges i rådets beslut 2008/633/RIF om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott. Uppgifterna ska begäras via centralkriminalpolisen eller skyddspolisen.

4 §

Vite

Polisen kan ålägga den av vilken polisen har rätt att få uppgifter som avses i 1 § 1 mom. 16 punkten att lämna uppgifterna inom en skälig tid. Polisen kan förena åläggandet med vite. Beslutet om föreläggande av vite ska iakttas även om ändring i beslutet söks. Vite får dock inte föreläggas om det finns skäl att misstänka någon för brott och det begärda materialet har samband med brottsmisstanken. På verkställigheten av vite tillämpas viteslagen (1113/1990).

4 kap.

Utlämnande av personuppgifter ur polisens informationssystem

1 §

Utlämnande av personuppgifter till en sådan behörig myndighet som avses i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten

Trots sekretessbestämmelserna får polisen genom teknisk anslutning eller som en datamängd lämna ut personuppgifter till Tullen och Gränsbevakningsväsendet när dessa behandlar personuppgifter för det ändamål som föreskrivs i 1 § 1 mom. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

Trots sekretessbestämmelserna får polisen genom teknisk anslutning eller som en datamängd lämna ut personuppgifter för sådana ändamål med behandlingen som avses i 1 mom. även när det är fråga om utlämnande av personuppgifter till

1) åklagare i den utsträckning som föreskrivs i 25 § i lagen om åklagarväsendet (439/2011),

2) domstolar för uppföljning av efterlysningar,

3) Rättsregistercentralen för uppföljning av efterlysningar, ansökningar om erkännande och verkställighet som ska sändas till en annan EU-stat samt för identifiering av finska medborgare,

4) Brottspåföljdsmyndigheten för ett i lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten avsett utlåtande till domstol om förutsättningarna för utdömande av samhällspåföljd, för verkställigheten av en samhällspåföljd, uppföljning av efterlysningar och beslut om besöksförbud som gäller dömda, placering av personer som dömts till ovillkorligt fängelsestraff, häktade och fångar, förhindande av kriminalitet under häktningstiden eller fängelsetiden, upprätthållande av säkerheten i fängelserna, bedömning av hot och avvärjande av dem och riktande av nödvändiga åtgärder för att nå dessa mål, för behandling av tillståndsärenden i anslutning till verkställigheten av påföljder och för övervakning av att tillståndsvillkoren iakttas, och

5) justitieförvaltningsmyndigheterna och militärmyndigheterna för uppföljning av deras egna efterlysningar.

2 §

Utlämnande av personuppgifter till andra myndigheter

Trots sekretessbestämmelserna får polisen genom teknisk anslutning eller som en datamängd lämna ut personuppgifter som behövs för att utföra en uppgift som i lag föreskrivits för en myndighet enligt följande:

1) till Trafiksäkerhetsverket uppgifter som avses i 11 § 1 mom. 5 punkten i lagen om fordonstrafikregistret samt, för bedömningen av förutsättningarna för att bevilja, förnya och återkalla ett tillstånd, de uppgifter som avses i 48 § i luftfartslagen (1194/2009),

2) till Nödcentralsverket, för utförande av de uppdrag som anges i 19 § 1 mom. i lagen om nödcentralsverksamhet (692/2010), uppgifter som behövs för att säkerställa förberedande åtgärder eller arbetarskyddet eller för att stödja enheten i fråga, med beaktande av vad som föreskrivs om begränsning av rätten att få information i 19 § 2 mom. i den lagen, samt för registrering i nödcentralsdatasystemet sådan säkerhetsinformation som avses i 2 kap. 2 § 5 mom. i denna lag,

3) till räddningsmyndigheterna för räddningsverksamhet som avses i 32 § i räddningslagen (379/2011),

4) till gränsbevakningsväsendet för gränskontroll och upprätthållande av gränssäkerheten, för förordnande av en värnpliktig till utbildning och en uppgift samt för anordnande av tjänstgöring, för skötsel av sådana förundersökningsuppgifter och uppgifter för förebyggande och avslöjande av brott som avses i lagen om militär disciplin och brottsbekämpning inom för-

svarsmakten (255/2014), för befordran till militär grad och belöning och skötsel av territorialövervakningsuppgifter, för andra sådana uppdrag som motsvarar de uppdrag för vilka uppgifterna har samlats in och registrerats för samt för andra ändamål i de fall som avses i 2 kap. 11 § 1 mom.,

5) till försvarsmakten för förordnande av en värnpliktig till utbildning och en uppgift samt för anordnade av tjänstgöring, förordnande till krishanteringsuppdrag och anordnande av krishanteringstjänstgöring, skötsel av militära underrättelseuppgifter, skötsel av territorialövervakningsuppgifter, skötsel av sådana förundersökningsuppgifter och uppgifter för förebyggande och avslöjande av brott som avses i lagen om militär disciplin och brottsbekämpning inom försvarsmakten, för befordran till militär grad och belöning samt för säkerhetsutredningar enligt säkerhetsutredningslagen (726/2014),

6) till socialmyndigheterna för behandling av ärenden som gäller en utlännings försörjning,

7) till Tullen för tullövervakning, skattekontroll, övervakning av personers in- och utresa och för utförande av den gränskontroll som ingår i detta, för Tullens övriga uppdrag som motsvarar de uppdrag för vilka uppgifterna samlats in och registrerats för samt för andra ändamål i de fall som avses i 2 kap. 11 § 1 mom. samt för stämning och annan delgivning,

8) till arbetsmyndigheterna för behandling av ärenden som gäller beviljande av uppehållstillstånd för arbetstagare eller uppehållstillstånd för näringsidkare eller övervakning av arbete,

9) till utrikesministeriet och finska beskickningar för behandling av ärenden som hör till deras behörighet och som gäller pass eller något annat resedokument, visum, uppehållstillstånd för arbetstagare, uppehållstillstånd för näringsidkare eller något annat uppehållstillstånd,

10) till Migrationsverket för behandling och avgörande av sådana ärenden avseende utlänningar och finskt medborgarskap som enligt lag eller förordning hör till Migrationsverket,

11) till domstolarna för behandling av ärenden som gäller skjutvapen, vapendelar, patroner eller särskilt farliga projektiler,

12) till en utmätningsman i enlighet med 3 kap. 67 § i utsökningsbalken (705/2007) för utsökningsutredningar eller annan verkställighet av utsökningsärenden,

13) till en tjänsteman som nämns i 1 eller 6 § i lagen om stämningsmän (505/1986) för stämning till en rättegång för bestämmande av förvandlingsstraff samt till stämningsmän för delgivning av stämning behövliga personuppgifter, uppgifter om säkerhet i arbetet och uppgifter om anhållna i informationssystemet för polisärenden,

14) till Forststyrelsens jakt- och fiskeövervakare för jakt- och fiskeövervakning som hör till deras behörighet,

15) till kommuner som är väghållare och Trafikverket uppgifter om trafikolyckor för främjande av trafiksäkerheten,

16) till arbetarskyddsförvaltningen för övervakning av förarnas kör- och vilotider uppgifter enligt Europaparlamentets och rådets direktiv 2006/22/EG om minimivillkor för genomförande av rådets förordningar (EEG) nr 3820/85 och (EEG) nr 3821/85 om sociallagstiftning på vägtransportområdet samt om upphävande av rådets direktiv 88/599/EEG,

17) till magistraten för uppgifter som avses i 38 § i medborgarskapslagen (359/2003),

18) till försvarsmakten, Tullen, gränsbevakningsväsendet och fångvårdsmyndigheterna för bedömning av om en hos dessa anställd med rätt att bära skjutvapen i sina tjänste- eller arbetsuppdrag är lämplig att bära skjutvapen.

Utöver vad som föreskrivs i 1 mom. får polisen trots sekretessbestämmelserna till en annan myndighet lämna ut sådana personuppgifter som är nödvändiga för att ett visst uppdrag som hör till myndigheten i fråga eller polisen ska kunna fullgöras, om det är uppenbart att utlämnandet av uppgifterna inte medför väsentlig olägenhet för de intressen som sekretessen är avsedd att skydda.

Trots sekretessbestämmelserna får polisen lämna ut i 2 kap. 11 § 4 mom. avsedda fingeravtrycksuppgifter i pass endast till de myndigheter som avses i 1 mom. 4, 7, 9 och 10 punkten i denna paragraf för styrkande av identitet och konstaterande av ett dokuments äkthet, när det behövs för behandling av ärenden som gäller en persons inresa, vistelse i landet eller utresa.

Innan personuppgifter lämnas ut ska mottagaren av uppgifterna för den personuppgiftsansvarige lägga fram en tillförlitlig utredning om att de skyddas på behörigt sätt.

Kvaliteten på de uppgifter som lämnas ut ska i den mån det är möjligt bekräftas och uppgifterna ska vid behov förses med information som gör det möjligt för mottagaren att bedöma hur korrekta, fullständiga, aktuella och tillförlitliga uppgifterna är. Om det framgår att felaktiga uppgifter har lämnats ut eller att uppgifter lämnats ut i strid med lag, ska detta utan dröjsmål meddelas mottagaren.

3 §

Utlämnande av personuppgifter till privata sammanslutningar och personer

Polisen får lämna ut personuppgifter till privata sammanslutningar och personer (*mottagare*) om detta är nödvändigt på grund av att saken är brådskande, att det är fråga om en farosituation, för att brott ska kunna förebyggas, egendom ska kunna återställas till ägaren eller av skäl som har samband med utredningen och utlämnandet av uppgifterna inte strider mot den registrerades legitima intresse.

För att allmänheten ska kunna underrättas och tips från allmänheten ska kunna fås får polisen via allmänt datanät lämna ut uppgifter som måste tillkännages särskilt på grund av att saken är brådskande, att det är fråga om en farosituation, för att brott ska kunna förebyggas, egendom ska kunna återställas till ägaren eller av skäl som har samband med utredningen, om utlämnandet av uppgifterna inte strider mot den registrerades legitima intresse.

På utlämnande av personuppgifter till en privat sammanslutning som är etablerad i ett tredjeland tillämpas bestämmelserna i 44 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

4 §

Utlämnande av personuppgifter till privata sammanslutningar eller näringsidkare via e-tjänster

Polisen får trots sekretessbestämmelserna lämna ut sådana uppgifter om giltigheten av tillstånd som behandlas för de ändamål som anges i 2 kap. 9 § till en privat sammanslutning eller en näringsidkare, om uppgifterna är nödvändiga för utförande av en uppgift som i lag föreskrivs för sammanslutningen eller näringsidkaren i fråga. Via e-tjänster får uppgifter lämnas ut endast som enskilda sökningar.

Utlämnande av uppgifter inom Europeiska unionen och Europeiska ekonomiska samarbetsområdet

5 §

Utlämnande av personuppgifter till tillsynsmyndigheter i Europeiska unionens medlemsstater

Polisen får trots sekretessbestämmelserna lämna ut de personuppgifter som avses i 2 kap. 3-6 § och 9 § till en behörig myndighet i en annan medlemsstat i Europeiska unionen som behandlar personuppgifterna för ett ändamål som anges i 1 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, under samma förutsättningar som polisen själv får behandla personuppgifterna i fråga. Personuppgifter som registrerats för att de uppdrag som avses i 1 kap. 1 § 2 mom. i polislagen ska kunna utföras får dock lämnas ut för ändamålet i fråga endast om uppgifterna är nödvändiga för utförande av det uppdrag för vilket de har samlats in och registrerats. Personuppgifterna får lämnas elektroniskt eller som en datamängd.

Utöver vad som föreskrivs i denna lag och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten ska på utlämnande av personuppgifter till de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater tillämpas lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009).

6 §

Utlämnande av personuppgifter ur det nationella systemet inom Schengens informationssystem

Bestämmelser om polisens rätt att trots sekretessbestämmelserna lämna ut uppgifter till de behöriga Schengenmyndigheterna ur det i 1 kap. 3 § avsedda nationella systemet inom Schengens informationssystem finns i författningsgrunden för Schengens informationssystem.

7 §

Utlämnande av personuppgifter till Schengenstater och Schengens informationssystem

Polisen får trots sekretessbestämmelserna lämna ut uppgifter om efterlysningar till Schengenstaternas behöriga myndigheter och för registrering i Schengens informationssystem. Bild- och fingeravtrycksuppgifter i anslutning till efterlysningar överförs via det nationella systemet inom Schengens informationssystem. Den tilläggsinformation som avses i författningsgrunden för Schengens informationssystem ska lämnas ut genom förmedling av Sirenekontoret.

8 §

Utlämnande av uppgifter till Europols informationssystem

Bestämmelser om polisens rätt att lämna ut personuppgifter som avses i 2 kap. 3–5 och 9 § till de informationssystem som används till i kapitel IV i Europolförordningen avsedd behandling av uppgifter finns i Europolförordningen. Det får sättas begränsningar för användningen av de personuppgifter som lämnas ut eller för vidare överlåtelse av personuppgifterna.

De personuppgifter som avses i 1 mom. får lämnas ut via den nationella enhet som avses i 2 § i lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning (214/2017) eller så kan polisen lämna ut personuppgifterna direkt i enlighet med 3 § i den lagen.

Centralen för utredning av penningstvätt vid centralkriminalpolisen har rätt att lämna ut personuppgifter till Europol inom ramen för sina uppdrag enligt 2 § i lagen om centralen för utredning av penningtvätt (445/2017).

9 §

Utlämnande av personuppgifter till Eurodacsystemet

Bestämmelser om polisens rätt att lämna ut fingeravtrycksuppgifter och andra personuppgifter ur sina informationssystem till Eurodacsystemet för jämförelse av fingeravtrycksuppgifter med uppgifter i det centrala systemet finns i Eurodacförordningen. Centralkriminalpolisen är den utsedda myndighet för brottsbekämpande ändamål som avses i artikel 5.1 i den förordningen.

10 §

Utlämnande av personuppgifter med stöd av Prümfördraget och Prümrådsbeslutet

På utlämnande på basis av en sökning som lett till en träff av DNA-uppgifter, fingeravtryckuppgifter och fordonsregisteruppgifter med stöd av fördraget mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (FördrS 54/2007), nedan *Prümfördraget*, och med stöd av rådets beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, nedan *Prümrådsbeslutet*, tillämpas artiklarna 3, 9 och 12 i Prümrådsbeslutet.

Utöver vad som föreskrivs i artiklarna 5, 10 och 14 i Prümrådsbeslutet ska 5 § i denna lag tillämpas på utlämnande av personuppgifter efter den uppgift om träff som avses i 1 mom.

11 §

Utlämnande av personuppgifter till tredjeland eller till den internationella kriminalpolisorganisationen

För förebyggande, utredning och avslöjande av brott får polisen lämna ut personuppgifter som avses i 2 kap. 3–5 och 9 § till den internationella kriminalpolisorganisationen (I.C.P.O. - Interpol) eller till polismyndigheter eller andra myndigheter i medlemsstater som inte hör till Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och vilka har till uppgift att skydda den nationella säkerheten, trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet eller att förebygga och utreda brott och föra brott till åtalsprövning, om uppgifterna är nödvändiga för utförande av uppdragen.

Trots sekretessbestämmelserna får polisen lämna ut personuppgifter som avses i 2 kap. 3–5 och 9 § till polismyndigheter eller andra myndigheter i ett annat tredjeland än ett som avses i 1 mom. och vilka har till uppgift att skydda den nationella säkerheten, trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet eller att förebygga och utreda brott och föra brott till åtalsprövning, om uppgifterna är nödvändiga för att

1) förebygga, avslöja eller utreda ett brott på vilket kan följa fängelse, eller för att lagföra ett sådant brott,

2) avvärja allvarlig fara som omedelbart hotar den allmänna säkerheten,

3) trygga den nationella säkerheten.

Det får sättas begränsningar och ställas villkor för användningen av de personuppgifter som lämnas ut. Polisen kan vägra lämna ut uppgifter om det kan vara till skada för arbetet med att förhindra, avslöja eller utreda brott eller föra brott till åtalsprövning, eller av någon annan grundad anledning.

Personuppgifterna får lämnas ut till myndigheterna i ett tredjeland eller till den internationella kriminalpolisorganisationen elektroniskt eller som en datamängd. Bestämmelser om internationell rättshjälp utfärdas särskilt.

12 §

Utlämnande av personuppgifter till tredjeland eller till den internationella kriminalpolisorganisationen i överensstämmelse med det ursprungliga ändamålet med behandlingen

Trots sekretessbestämmelserna får personuppgifter lämnas ut till de behöriga myndigheter som avses i internationella avtal eller andra arrangemang som gäller återtagande av personer

som olagligen kommit in och vistas i landet för utförande av de uppdrag som avses i de internationella avtalen eller arrangemangen.

I 2 kap. 11 § 4 mom. avsedda fingeravtrycksuppgifter i pass får lämnas ut endast på det sätt som föreskrivs i momentet i fråga.

Trots sekretessbestämmelserna får det till de myndigheter som ansvarar för vapentillsynen i en annan stat lämnas ut uppgifter ur polisens personregister om förvärv, innehav, överföring, införsel och utförsel av skjutvapen, vapendelar, patroner och särskilt farliga projektiler, om det med tanke på vapentillsynen är nödvändigt att lämna ut och få uppgifterna.

13 §

Behandling av personuppgifter som fåtts från ett tredjeland, den internationella kriminalpolisorganisationen eller någon annan internationell brottsbekämpande myndighet

Vid behandlingen av personuppgifter som fåtts från ett tredjeland, den internationella kriminalpolisorganisationen eller någon annan internationell brottsbekämpande myndighet ska i fråga om sekretess, tystnadsplikt, begränsningar i användningen av personuppgifter, vidare överlåtelse av personuppgifter eller återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna ställt.

Om inget annat följer av 1 mom., får polisen använda personuppgifter som den mottagit för andra ändamål än de som uppgifterna lämnades ut för, om de är nödvändiga för att

1) förebygga, avslöja eller utreda ett brott på vilket kan följa fängelse, eller för att lagföra ett sådant brott,

2) avvärja allvarlig fara som omedelbart hotar den allmänna säkerheten,

3) trygga den nationella säkerheten, eller

4) genomföra ett rättsligt eller administrativt förfarande som har direkt samband med åtgärder för att förebygga, utreda eller väcka åtal för ett annat brott eller verkställa straffrättsliga påföljder.

14 §

Beslut om utlämnande av uppgifter

Beslut om rätten att lämna ut uppgifter ur polisens personregister till myndigheter som avses i 1 och 2 § och om rätten för de myndigheter som avses i 3 kap. att lämna ut uppgifter till polisens informationssystem som en datamängd eller genom teknisk anslutning fattas av den personuppgiftsansvarige eller av en annan polisenhet som den personuppgiftsansvarige har förordnat till uppdraget.

När beslut om utlämnande fattas ska uppgifternas art beaktas för att datasekretessen och den registrerades datasäkerhet ska kunna tryggas.

5 kap.

Utplåning, kontroll och arkivering av personuppgifter

1 §

Utplåning av personuppgifter som anknyter till brottmål

Uppgifterna i ett brottmål som överförts till en åklagare för avgörande ska utplånas

1) när fem år har förflutit sedan brottmålet överfördes till åklagaren, om det grövsta misstänkta brottet i brottmålet kan leda till böter,

2) när tio år har förflutit sedan brottmålet överfördes till åklagaren, om det grövsta misstänkta brottet i brottmålet kan leda till ett fängelsestraff på högst fem år,

3) när tjugo år har förflutit sedan brottmålet överfördes till åklagaren, om det grövsta misstänkta brottet i brottmålet kan leda till fängelse i över fem år.

Uppgifterna i övriga brottmål ska utplånas när ett år har förflutit sedan åtalsrätten för det senaste misstänkta brottet preskriberats, dock tidigast när fem år har förflutit sedan brottmålet registrerades.

De uppgifter som avses i 1 och 2 mom. utplånas inte, om åtalsrätten inte har preskriberats.

Signalement och andra personuppgifter som registrerats för identifiering av personer som misstänks för brott, för utredning av brott och för registrering av gärningsmän ska utplånas senast när tio år har förflutit sedan den sista uppgiften om den som är misstänkt för brottet infördes. Uppgifterna ska dock utplånas senast tio år efter den registrerades död, om det strängaste föreskrivna straffet för det grövsta brott som använts som grund för registrering är fängelse i minst ett år. Uppgifterna utplånas senast när fem år har förflutit sedan anteckningen infördes, om det i samband med undersökning framgår att inget brott har begåtts.

Logguppgifterna och övervakningsuppgifterna om sådan behandling av uppgifter som grundar sig på Prümfördraget och Prümrådsbeslutet lagras och utplånas i enlighet med bestämmelserna i artikel 39.4 och 39.5 i Prümfördraget och artikel 30.4 och 30.5 i Prümrådsbeslutet.

De i 1–3 mom. avsedda personuppgifter som anknyter till brottmål får dock fortfarande bevaras, om de behövs för att behandla ett ärende, utföra ett uppdrag eller för att trygga de rättigheter som den registrerade, någon annan part eller en person som hör till polispersonalen har. Behovet av att bevara personuppgifterna ska bedömas minst vart tredje år.

Trots vad som i 1–3 mom. föreskrivs om utplåning av uppgifter ska uppgifter om registrerade som var under 15 år gamla då de begick brottet utplånas när den registrerade fyller 18 år, om inte den registrerade har gjort sig skyldig till en brottslig gärning efter att ha fyllt 15 år. Uppgifterna ska dock inte utplånas på denna grund, om brottmålet gäller andra misstänkta för den brottsliga gärningen och uppgifterna om dem ännu inte utplånas eller om någon av anteckningarna gäller en brottslig gärning för vilken inte föreskrivs någon annan påföljd än fängelse.

2 §

Utplåning av personuppgifter som behandlas för andra i 2 kap. 3 och 5 § avsedda ändamål

Personuppgifter som behandlas för andra i 2 kap. 3 och 5 § avsedda ändamål ska utplånas när fem år har förflutit sedan anmälan eller ärendet registrerades, om inte de hänför sig till ett brottmål som undersöks. Säkerhetsinformation ska dock utplånas senast ett år efter den registrerades död.

Av uppgifterna om efterlysningar av personer ska med avvikelse från 1 mom. uppgifter om näringsförbud utplånas när fem år förflutit sedan näringsförbudet upphörde, uppgifter om besöksförbud när fem år har förflutit sedan besöksförbudet meddelades, uppgifter om övervakad frihet på prov eller övervakningsstraff när fem år har förflutit sedan den övervakade friheten på prov eller övervakningsstraffet avtjänats och andra uppgifter när tre år har förflutit sedan efterlysningen eller förbudet återkallades eller upphörde.

Uppgifter om informationskälla ska utplånas när tio år har förflutit sedan den sista uppgiften infördes.

Uppgifter för identifiering av utlänningar ska utplånas när tio år har förflutit sedan anteckningen infördes. Om en registrerad har beviljats finskt medborgarskap, ska uppgifterna för identifiering av utlänningen dock utplånas när ett år har förflutit sedan den personuppgiftsansvarige fått kännedom om medborgarskapet. Alla uppgifter för identifiering av en utlänning ska dock utplånas senast ett år efter den registrerades död, om det inte finns särskilda skäl att fortfarande bevara dem för att behandla ett ärende, utföra ett uppdrag eller för att trygga de

rättigheter som den registrerade, någon annan part eller en person som hör till polispersonalen har. Behovet av att bevara personuppgifterna ska bedömas minst vart femte år.

3 §

Utplåning av personuppgifter som anknyter till kriminalunderrättelseinhämtning och av observationsuppgifter

Personuppgifter som anknyter till kriminalunderrättelseinhämtning ska utplånas senast när tio år har förflutit sedan den sista uppgiften om brottet, den brottsliga verksamheten eller uppdraget infördes i informationssystemet, om det inte finns särskilda skäl att fortfarande bevara dem för att behandla ett ärende, utföra ett uppdrag eller för att trygga de rättigheter som den registrerade, någon annan part eller en person som hör till polispersonalen har. Behovet av att bevara personuppgifterna ska bedömas minst vart femte år.

Observationsuppgifter ska utplånas senast när sex månader har förflutit sedan anteckningen infördes i informationssystemet.

Personuppgifter som behandlas i enlighet med 2 kap. 7 § 2 mom. i syfte att utreda om uppgifterna är betydelsefulla ska utplånas senast när sex månader har förflutit sedan anteckningen infördes i informationssystemet. Bild- och ljudupptagningar som gjorts med hjälp av tekniska hjälpmedel ska dock utplånas senast när 96 timmar har förflutit sedan anteckningen infördes i informationssystemet.

4 §

Utplåning av personuppgifter som behandlas för utförande av tillståndsförvaltnings- och tillsynsuppgifter och uppgifter enligt hittegodslagen

Personuppgifter som behandlas för utförande av tillståndsförvaltnings- och tillsynsuppgifter ska utplånas senast när tjugo år har förflutit sedan beslutet fattades eller förföll eller den i beslutet angivna giltighetstiden gick ut eller personuppgiften infördes.

Med avvikelse från 1 mom.

1) ska uppgifterna i en skjutvapenanmälan enligt skjutvapenlagen utplånas senast när tre år har förflutit sedan uppgiften infördes,

2) ska uppgifterna om ägaren eller innehavaren av vapen eller ett annat föremål som registrerats enligt skjutvapenlagen utplånas när trettio år har förflutit sedan föremålet gjordes varaktigt obrukbart, skrotades eller fördes varaktigt ut ur landet,

3) ska personuppgifter som anknyter till hittegodsverksamhet utplånas senast när ett år har förflutit sedan uppgiften infördes,

4) ska personuppgifter som ingår i sådana rapporter om misstanke om överträdelser som avses i 7 kap. 9 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism utplånas i enlighet med bestämmelserna i 2 mom. i den paragrafen samt övriga personuppgifter som anknyter till tillsyn enligt det kapitlet senast när fem år har förflutit sedan anteckningen infördes.

5) ska personuppgifter som ska behandlas för övervakning enligt lotterilagen eller lagen om förhindrande av penningtvätt och av finansiering av terrorism och som gäller kunder hos en i de lagarna avsedd penningspelssammanslutning, näringsidkare eller sammanslutning som ska övervakas utplånas genast när de inte längre behövs för utförande av tillsynsuppdraget.

De personuppgifter som avses i 1 mom. och 2 mom. 1 punkten ska dock utplånas senast ett år efter den registrerades död, om det inte finns särskilda skäl att fortfarande bevara dem. Behovet av att bevara personuppgifterna ska bedömas minst vart femte år.

5 §

Uppgifter som konstaterats vara felaktiga

Trots bestämmelserna om rättelse av en oriktig uppgift i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och i dataskyddsförordningen, får en uppgift som konstaterats vara felaktig bevaras tillsammans med den korrigerade uppgiften, om det behövs för att trygga de rättigheter som den registrerade, någon annan part eller en person som hör till polispersonalen har. En sådan uppgift får användas endast i det syfte som här avses.

En uppgift som har konstaterats vara felaktig får dock inte bevaras i det nationella systemet inom Schengens informationssystem.

En uppgift som konstaterats vara felaktig och som bevaras med stöd av 1 mom. ska utplånas genast när den inte längre behövs för att trygga rättigheterna, dock senast när fem år har förflutit sedan den föreskrivna tiden för utplåning av uppgiften gått ut.

6 §

Arkivering av uppgifter

I fråga om arkivfunktionens uppgifter och om handlingar som ska arkiveras gäller vad som föreskrivs i arkivlagen (831/1994) eller i bestämmelser eller föreskrifter som utfärdats med stöd av den.

6 kap.

Den registrerades rättigheter

1 §

Tillgodoseende av den registrerades rätt till insyn

I syfte att tillgodose den registrerade rätt till insyn enligt 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och den registrerades rätt till tillgång till uppgifter enligt artikel 15 i dataskyddsförordningen lämnar den personuppgiftsansvarige ut de behövliga personuppgifterna och andra uppgifter för utövande av insyn, om inte den personuppgiftsansvarige har förordnat någon annan polisenhet att lämna ut uppgifterna.

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd polisenhet samt styrka sin identitet. En begäran kan också framställas genom att en tillförlitlig elektronisk identifiering används.

2 §

Inskränkningar i rätten till insyn

Med avvikelse från 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten gäller rätten till insyn inte

1) personuppgifter som avses i 2 kap. 4 §, observationsuppgifter som avses i 6 § och personuppgifter som avses i 7 § 2 mom.,

2) personuppgifterna om hemlig övervakning och särskild kontroll i Schengens informationssystem,

3) uppgifter om kriminalunderrättelseinhämtning, klassificering eller informationskälla i fråga om en person eller en gärning eller uppgifter som används för brottsanalys och teknisk undersökning av brott,

5) uppgifter som fåtts genom de inhämtningsmetoder som avses i 5 kap. i polislagen och 10 kap. i tvångsmedelslagen samt med stöd av 19 kap. 157 § i informationssamhällsbalken.

Den registrerades rätt till insyn kan i fråga om de ändamål med behandlingen som anges i 2 kap. 9 § inskränkas endast i enskilda fall, om det med beaktande av den registrerades rättigheter är proportionerligt och nödvändigt på de grunder som anges i artikel 23.1 i dataskyddsförordningen.

Den registrerade har rätt att utöva sina rättigheter i de situationer som avses i 1 och 2 mom. på det sätt som föreskrivs i 29 § i lagen om behandling av personuppgifter i brott mål och i samband med upprätthållandet av den nationella säkerheten.

3 §

Utövande av rätten till insyn i den datafil som upprätthålls av den tekniska stödfunktionen i Schengens informationssystem

Utöver bestämmelserna i 1 § har var och en rätt att begära att den tillsynsmyndighet som avses i artikel 115 i Schengenkonventionen kontrollerar att insamlingen, registreringen, behandlingen och användningen av personuppgifter som gäller honom eller henne i den datafil som upprätthålls av den tekniska stödfunktionen i Schengens informationssystem sker på ett lagligt och riktigt sätt. Begäran om detta ska framställas till Dataskyddsmyndigheten eller en polisinrättning. En begäran om kontroll som framställts hos polisinrättningen ska utan dröjsmål överföras till Dataskyddsmyndigheten.

En i 1 mom. avsedd begäran om kontroll hos en polisinrättning ska framställas personligen hos polisinrättningen, och den som framställer begäran ska samtidigt styrka sin identitet.

4 §

Utövande av rätten till insyn i fråga om behandlingen av personuppgifter som grundar sig på Prümfördraget och Prümrådsbeslutet

Utöver bestämmelserna i 1 § har den registrerade rätt att begära Dataskyddsmyndigheten kontrollera att den behandling av personuppgifter om honom eller henne som grundar sig på Prümfördraget och Prümrådsbeslutet är lagenlig.

7 kap.

Skyddspolisens behandling av personuppgifter

1 §

Tillämpningsområde

På behandlingen av skyddspolisens personuppgifter tillämpas lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten, med undantag av 7 kap. i den lagen, om inte något annat föreskrivs i detta kapitel. (På behandlingen av skyddspolisens personuppgifter tillämpas inte dataskyddslagen (/).)

2 §

Registerföring

Skyddspolisen är personuppgiftsansvarig för de personuppgifter som avses i detta kapitel.

3 §

Skyddspolisens behandling av personuppgifter

Skyddspolisen får behandla personuppgifter som behövs för att skydda den nationella säkerheten samt för att förhindra, avslöja och utreda verksamhet, projekt och brott som hotar stats- och samhällsordningen eller statens säkerhet.

Personuppgifterna får behandlas på det sätt som föreskrivs i 2 kap. 1 och 2 §.

Skyddspolisen får behandla personuppgifter som gäller särskilda kategorier av personuppgifter och som är nödvändiga för att skyddspolisen ska kunna utföra sina uppdrag.

Bestämmelser om personuppgifter som behandlas med avseende på säkerhetsutredningar utfärdas särskilt.

4 §

Behandling av personuppgifter för bedömning av deras betydelse

Skyddspolisen får på beslut av en polisman som hör till befälet behandla personuppgifter som fåtts i samband med ett uppdrag och som kan vara av betydelse för skyddandet av den nationella säkerheten, för att klarlägga om uppgifterna behövs för sådana ändamål med behandlingen som föreskrivs i 3 §.

5 §

Utlämnande av personuppgifter

Skyddspolisen får till andra myndigheter eller sammanslutningar som sköter offentliga uppdrag trots sekretessbestämmelserna lämna ut personuppgifter som skyddspolisen behöver för att utföra sina uppdrag.

Skyddspolisen får trots sekretessbestämmelserna lämna ut personuppgifter till andra polisenheter för att ett uppdrag som föreskrivs för dem ska kunna utföras samt till andra myndigheter eller sammanslutningar som sköter offentliga uppdrag på det sätt som anges i 4 kap.

Skyddspolisen får trots sekretessbestämmelserna lämna ut personuppgifter till privata sammanslutningar och personer när det är nödvändigt för att skyddspolisen ska kunna utföra sina uppdrag.

Personuppgifterna får lämnas ut elektroniskt eller som en datamängd.

6 §

Utlämnande av personuppgifter i samband med internationellt samarbete

Skyddspolisen får för att kunna utföra sina uppdrag trots sekretessbestämmelserna lämna ut personuppgifter till utländska säkerhets- och underrättelsetjänster och till utländska myndigheter som har till uppgift att skydda den nationella säkerheten, trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet eller att förebygga och utreda brott och föra brott till åtalprövning samt till internationella kriminalpolisorganisationer (Europol och I.C.P.-Interpol).

Personuppgifterna får lämnas ut elektroniskt eller som en datamängd.

7 §

Rätt att få information

Skyddspolisen har rätt att på det sätt som anges i 3 kap. få information för att skydda den nationella säkerheten.

8 §

Behandling av personuppgifter som fåtts i samband med internationellt samarbete.

Vid behandlingen av personuppgifter som fåtts från utländska säkerhets- och underrättelsetjänster ska i fråga om sekretess, tystnadsplikt, begränsningar i användningen av uppgifter, vidare överlåtelse av uppgifter eller återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna ställt.

9 §

Skyddspolisens rätt att förvalta sitt informationssystem

Om den personuppgiftsansvarige trots sekretessbestämmelserna har i en annan lag föreskriven rätt att ur sitt personregister genom en teknisk anslutning eller som en datamängd lämna ut uppgifter till polisen, får Skyddspolisen för att förvalta sitt informationssystem jämföra uppgifterna i personregistret i fråga med innehållet i sitt informationssystem. Onödiga uppgifter ska utplånas utan dröjsmål efter det att jämförelsen har gjorts. Vid registrering av personuppgifter ska det säkerställas att onödiga personuppgifter inte registreras i informationssystemet.
Skyddspolisen har rätt att få uppgifterna avgiftsfritt.

10 §

Inskränkningar i rätten till insyn

Det finns ingen rätt till insyn i personuppgifter som behandlas av Skyddspolisen med stöd av 3 och 4 §.
Den registrerade har rätt att utöva sina rättigheter i de situationer som avses i 1 mom. på det sätt som föreskrivs i 29 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

11 §

Utplåning av uppgifter

Alla uppgifter om personer som registrerats med stöd av 3 § ska utplånas senast när 25 år har förflutit sedan den sista uppgiften infördes, om det inte finns särskilda skäl att fortfarande bevara dem för att behandla ett ärende, utföra ett uppdrag eller för att trygga de rättigheter som den registrerade, någon annan part eller en person som hör till Skyddspolisens personal har. Behovet av att bevara personuppgifterna ska bedömas minst vart femte år.
De uppgifter om personer som registrerats med stöd av 4 § ska utplånas senast när sex månader har förflutit sedan uppgiften infördes.

12 §

Arkivering av uppgifter

I fråga om arkivfunktionens uppgifter och om handlingar som ska arkiveras gäller vad som föreskrivs i arkivlagen (831/1994) eller i bestämmelser eller föreskrifter som utfärdats med stöd av den.

8 kap.

Särskilda bestämmelser

1 §

Skydd av känsliga personuppgifter

Vid registrering och annan behandling av sådana känsliga personuppgifter i elektronisk form som avses i 11 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och i artikel 9 i dataskyddsförordningen ska den personuppgiftsansvarige och tillsynsmyndigheten särskilt sörja för dataskyddet för dessa identifieringsuppgifter.

Vid registrering eller annan behandling av en persons känsliga uppgifter ska det ses till att

1) de informationssystem, maskinvaror och programvaror som används för identifiering och för behandling av personuppgifterna är säkra,

2) personuppgifterna är skyddade mot obehörig åtkomst och mot kränkningar, modifieringar och förfalskningar som avser personuppgifternas konfidentialitet och integritet samt annan behandling som sker av misstag eller i strid med lag, och

3) det vid identifiering och vid behandling av identifieringsuppgifter även i övrigt genomförs behövliga tekniska och organisatoriska åtgärder för att säkerställa att identifieringen och behandlingen kan genomföras på ett sätt som tryggar dataskyddet och integritetsskyddet.

Den personuppgiftsansvarige ska svara för det ovan avsedda dataskyddet också i fråga om en tredje part som på uppdrag av den personuppgiftsansvarige helt eller delvis registrerar känsliga personuppgifter. Den personuppgiftsansvarige svarar för att uppdragstagaren har samma skyldighet som den personuppgiftsansvarige att skydda uppgifterna och för att uppdragstagaren inte har någon annan rätt att behandla uppgifterna.

2 §

Personuppgiftsansvarig

Polisstyrelsen är personuppgiftsansvarig för de personuppgifter som polisen behandlar på nationell nivå.

3 §

Skyddsåtgärder i civilrättsliga frågor

Vad som i denna lag föreskrivs om behandlingen av personuppgifter som anknyter till besöksförbud ska tillämpas på skyddsåtgärder som anmälts till polisens register med stöd av 4 § i lagen om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor (227/2015).

4 §

Närmare bestämmelser och anvisningar

Närmare bestämmelser om förfaringssätten vid beslut om utlämnande av personuppgifter enligt 4 kap. 10 § och vid utövande av rätt till insyn enligt 8 kap. 2 § får utfärdas genom förordning av statsrådet.

Polisstyrelsen fastställer formulären för de blanketter som ska användas vid åtgärder som hör till polisen, om inte något annat föreskrivs i lagen.

5 §

Ikraftträdande

Denna lag träder i kraft den 2018 .

Genom denna lag upphävs lagen av den 1 oktober 2003 om behandling av personuppgifter i polisens verksamhet (761/2003) jämte ändringar.

2.

Lag

om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet

I enlighet med riksdagens beslut föreskrivs:

1 §

Tillämpningsområde

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, nedan *PNR-direktivet*.

2 §

Förhållande till annan lagstiftning

Utöver vad som föreskrivs i denna lag tillämpas lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/2018) tillämpas på behandling av passageraruppgifter.

3 §

Definitioner

I denna lag avses med

1) *lufttrafikföretag* ett lufttrafikföretag med giltig operativ licens eller motsvarande som ger företaget rätt att bedriva passagerarflygtrafik,

2) *flygning utanför Europeiska unionen* varje reguljär- eller charterflygning som utförs av ett lufttrafikföretag, med avgång från ett tredjeland och planerad landning på en medlemsstats territorium eller med avgång från en medlemsstats territorium och planerad landning i ett tredjeland, i båda fallen inklusive mellanlandningar på territorier i medlemsstater eller tredjeländer,

3) *flygning inom Europeiska unionen* varje reguljär- eller charterflygning som utförs av ett lufttrafikföretag, med avgång från en medlemsstats territorium och planerad landning på en eller flera andra medlemsstaters territorium, utan mellanlandningar på tredjeländers territorier,

4) *passagerare* de personer, inbegripet personer i transfer eller transit förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett luftfartyg med lufttrafikföretagets samtycke, vilket framgår av att personen finns med på passagerarförteckningen,

5) *passageraruppgiftssamling* (PNR, Passenger Name Record) en sammanställning av sådan reseinformation om varje enskild passagerare som de lufttrafikföretag som sköter bokning och de lufttrafikföretag som deltar i transporten behöver för att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning, oavsett om informationen finns i reservationssystemet, det avgångskontrollsystem som används för att checka in passagerare på flygningar eller i ett motsvarande system,

6) *reservationssystem* lufttrafikföretagets interna system där passageraruppgifter samlas för hantering av reservationer,

7) *terroristbrott* brott som avses i 34 a kap. 1–5 § i strafflagen (39/1889),

8) *grov brottslighet* sådana former av brott som avses i bilaga II till PNR-direktivet och för vilka det föreskrivna maximistraffet är fängelse i minst tre år,

9) *maskering* att göra de uppgifter som kan användas för att omedelbart identifiera en passagerare osynliga för en användare,

10) *behöriga myndigheter* i Finland polisen, Tullen och Gränsbevakningsväsendet,

11) *Europol* den byrå som avses i artikel 1.1 i Europaparlamentets och rådets förordning (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF, nedan *Europolförordningen*.

4 §

Lufttrafikföretags skyldighet att överföra passageraruppgifter

Ett lufttrafikföretag ska till den i 5 § avsedda enheten för passagerarinformation överföra passageraruppgifter enligt denna paragraf för de ankommande och avgående flygningar utanför eller inom Europeiska unionen som de utför, till den del uppgifterna har samlats in som en del av den normala affärsverksamheten. I fråga om flygningar med gemensam linjebeteckning gäller skyldigheten det företag som utför flygningen. Om lufttrafikföretaget också har samlat in sådan förhandsinformation om passagerare som avses i punkt 18 i bilaga I till PNR-direktivet, ska även denna information överföras. Lufttrafikföretaget ska överföra passageraruppgifterna avgiftsfritt.

De passageraruppgifter som avses i 1 mom. omfattar

1) passageraruppgiftssamlingens lokaliseringskod,

2) datum för bokning/utfärdande av biljett,

3) planerat/planerade resdatum,

4) namn,

5) adress och kontaktuppgifter,

6) alla former av betalningsinformation,

7) hela resrutten för den aktuella passageraruppgiftssamlingen,

8) uppgifter om bonusprogram,

9) resebyrå/resebyråtjänsteman,

10) passagerares resestatus, inbegripet resebekräftelser, incheckningsstatus, passagerare som inte infinner sig eller passagerare utan bokning,

11) delade passageraruppgifter,

12) allmänna anmärkningar,

13) biljettinformation,

14) platsnummer och annan platsinformation,

15) information om gemensam linjebeteckning,

16) all bagageinformation,

17) antal medresenärer i passageraruppgifterna och deras namn,

18) eventuell förhandsinformation som har samlats in om passagerare, samt

19) alla tidigare ändringar av de passageraruppgifter som avses i 1–18 punkten.

Passageraruppgifterna ska överföras 24 timmar före den planerade ankomst-eller avgångstiden för flygningen och omedelbart efter det att gatens dörrar stängts, varvid överföringen av uppgifter också kan begränsas till uppdateringar av tidigare överföringar. Om uppgifterna behövs för att man ska kunna reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska uppgifterna på begäran av enheten för passagerarinformation överföras även vid andra tidpunkter.

Vid överföring av passageraruppgifter ska de i artikel 16 i PNR-direktivet avsedda gemensamma protokoll och understödda dataformat som antagits genom kommissionens genomförandeakt användas.

5 §

Enhet för passagerarinformation

Den riksomfattande PTG-kriminalunderrättelseenhet som avses i 5 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009) är i denna lag avsedd enhet för passagerarinformation.

6 §

Behandling av passageraruppgifter

Enheten för passagerarinformation får behandla passageraruppgifter för identifiering av personer som kan vara delaktiga i terroristbrott eller grov brottslighet, enligt följande:

1) före passagerarnas beräknade ankomst eller avresa,

2) på motiverad begäran, som bygger på tillräckliga observationer, från de behöriga myndigheterna, enheten för passagerarinformation i en annan medlemsstat eller Europol, och

3) i enlighet med på förhand fastställda kriterier för bedömning och analys eller för att uppdatera kriterierna eller fastställa nya kriterier.

De i 1 mom. 3 punkten avsedda bedömningskriterierna, som enheten för passagerarinformation fastställer och i samarbete med de behöriga myndigheterna regelbundet ska se över, ska vara riktade, proportionella och tydliga. Bedömningskriterierna får inte grunda sig på uppgifter om en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, medlemskap i fackförbund, hälsotillstånd, sexualliv eller sexuella läggning.

Enheten för passagerarinformation får i samband med den behandling som avses i 1 mom. 1 punkten genom automatiserade metoder jämföra passageraruppgifter med

1) uppgifter som lagrats i syfte att trygga de behöriga myndigheternas brottsutredning och kriminalunderrättelseinhämtning samt rätts- och samhällsordningen och att upprätthålla allmän ordning och säkerhet, och

2) de personuppgifter som avses i 7 kap. 3 § i lagen om behandling av personuppgifter i polisens verksamhet (/) och som behandlas av skyddspolisen, samt

3) de uppgifter som lagrats i det i 1 kap. 3 § 2 punkten i lagen om behandling av personuppgifter i polisens verksamhet avsedda Schengens informationssystems och den internationella kriminalpolisorganisationens (I.C.P.O.-Interpol) databaser.

Eventuella träffar i samband med sådan behandling av passageraruppgifter som avses i 1 mom. 1 punkten ska granskas individuellt.

Jämförelse enligt 3 mom. 2 punkten ska genomföras på ett sätt som tryggar dataskyddet, i enlighet med vad som avtalas med skyddspolisen. Jämförelsen kan genomföras endast av en av skyddspolisen förordnad tjänsteman till enheten för passagerarinformation. De passageraruppgifter som observerats genom jämförelsen och resultaten av behandlingen av uppgifterna kan vidarebefordras endast med samtycke av skyddspolisen.

De passageraruppgifter som avses i denna paragraf får vid enheten för passagerarinformation behandlas endast av de tjänstemän till vars uppgifter det hör att behandla uppgifterna.

7 §

Utlämnande av passageraruppgifter till behöriga myndigheter

De passageraruppgifter om personer som har identifierats genom den behandling av passageraruppgifter som avses i 6 § 1 mom. 1 punkten eller resultaten av behandlingen av uppgifterna ska lämnas ut till de behöriga myndigheterna så att de kan utreda personernas delaktighet i terroristbrott eller grov brottslighet. Uppgifterna eller resultaten av behandlingen av uppgifterna får lämnas ut till de behöriga myndigheterna även på motiverad begäran som bygger på

tillräckliga observationer. De uppgifter som avses i detta moment får lämnas ut endast fall för fall. Dataskyddsombudet vid enheten för passagerarinformation ska ha åtkomst till passageraruppgiftssamlingen.

8 §

Utbyte av passageraruppgifter mellan medlemsstater

Enheten för passagerarinformation får begära passageraruppgifter av en enhet för passagerarinformation i en annan medlemsstat i syfte att förhindra terroristbrott eller andra grova brott. Begäran ska motiveras. Enheten för passagerarinformation ska till de behöriga myndigheterna lämna ut de passageraruppgifter eller de resultat av behandlingen av uppgifterna som den tagit emot av en enhet för passagerarinformation i en annan medlemsstat.

Enheten för passagerarinformation ska lämna ut uppgifterna om personer som den identifierat genom sådan behandling av passageraruppgifter som avses i 6 § 1 mom. 1 punkten till motsvarande enheter för passagerarinformation i andra medlemsstater. De uppgifter som lämnas ut ska omfatta alla relevanta och nödvändiga passageraruppgifter om personer som identifierats genom behandlingen eller resultaten av behandlingen av uppgifterna. Enheten för passagerarinformation får dessutom lämna ut passageraruppgifter eller resultaten av behandlingen av uppgifterna till en enhet för passagerarinformation i en annan medlemsstat på dennes motiverade begäran.

De behöriga myndigheterna kan direkt av en enhet för passagerarinformation i en annan medlemsstat begära passageraruppgifter när det behövs i nödfall eller för att bekämpa terrorism och grov brottslighet. Begäran ska motiveras och meddelande om den ska skickas till enheten för passagerarinformation i Finland. Under motsvarande förutsättningar får enheten för passagerarinformation i Finland lämna ut passageraruppgifter till de behöriga myndigheterna i en annan medlemsstat på deras begäran.

9 §

Överföring av passageraruppgifter till Europol

Enheten för passagerarinformation får på motiverad begäran överföra passageraruppgifter eller resultaten av behandlingen av uppgifterna till Europol för sådan behandling av uppgifterna som avses i kapitel IV i Europolförordningen i syfte att bekämpa terroristbrott och grov brottslighet när uppgifterna behöver överföras för att målen för medlemsstaternas behöriga myndigheters brottsbekämpningssamarbete och ömsesidiga samarbete i enlighet med artikel 3 i den förordningen ska nås.

10 §

Överföring av passageraruppgifter till tredjeländer

Enheten för passagerarinformation får överföra passageraruppgifter och resultaten av behandlingen av uppgifterna till ett tredjeland endast i enskilda fall, om

1) de bestämmelser om allmänna principer för överföring av personuppgifter till tredjeländer som finns i 7 kap. 41 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten iakttas, och

2) uppgifterna behöver överföras för att sådana terroristbrott och sådan grov brottslighet som avses i denna lag ska kunna bekämpas.

Om passageraruppgifter eller resultaten av behandlingen av uppgifterna vidareöverförs till ett annat tredjeland, är förutsättningen för överföringen utöver det som nämns i 1 mom. att det är nödvändigt att överföra uppgifterna i syfte att bekämpa sådana terroristbrott och sådan grov

brottslighet som avses i denna lag och att enheten för passagerarinformation har gett tillstånd till överföringen.

Med avvikelse från 1 mom. får passageraruppgifter som överförts från en enhet för passagerarinformation i en annan medlemsstat överföras till ett tredjeland utan tillstånd av enheten för passagerarinformation i medlemsstaten i fråga endast om överföringen är av väsentlig betydelse för att man ska kunna reagera på ett i denna lag avsett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller ett tredjeland och tillstånd inte kan fås i tid. Enheten för passagerarinformation i medlemsstaten i fråga ska informeras om överföringen och överföringen ska registreras på behörigt sätt och kontrolleras i efterhand.

Innan passageraruppgifter överförs till de behöriga myndigheterna i ett tredjeland ska enheten för passagerarinformation förvissa sig om att tredjelandets planerade användning av uppgifterna är förenlig med villkoren och skyddsåtgärderna enligt denna paragraf. Dataskyddsombudet vid enheten för passagerarinformation ska informeras om överföringen av uppgifterna.

11 §

Utplåning och maskering av passageraruppgifter och utlämnande av maskerade uppgifter

Passageraruppgifter som har överförts av ett lufttrafikföretag ska utplånas ur registret vid enheten för passagerarinformation när fem år har förflutit sedan de överfördes till enheten för passagerarinformation. När sex månader har förflutit sedan uppgifterna överfördes till enheten för passagerarinformation ska följande passageraruppgifter avskiljas från uppgifterna genom maskering:

1) namn, inklusive namn på andra passagerare i passageraruppgifterna samt antal passagerare som reser tillsammans,

2) adress och andra kontaktuppgifter,

3) alla former av betalningsinformation, inbegripet faktureringsadress, om denna innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgifterna avser eller andra personer,

4) uppgifter om bonusprogram,

5) allmänna anmärkningar, och

6) eventuell förhandsinformation som har samlats in om passagerare (API-uppgifter).

Enheten för passagerarinformation ska utplåna resultaten av den behandling som avses i 6 § 1 mom. 1 punkten när de behöriga myndigheterna eller vid behov en enhet för passagerarinformation i en annan medlemsstat har informerats om en träff. Om resultatet efter en granskning visar sig vara felaktigt får den felaktiga uppgiften, för att felaktiga träffar ska kunna undvikas i framtiden, bevaras till dess att uppgifterna har utplånats med stöd 1 mom. De behöriga myndigheter eller den enhet för passagerarinformation i en annan medlemsstat som resultaten av behandlingen lämnats ut till ska informeras om felaktiga resultat.

Om de passageraruppgifter som ett lufttrafikföretag har överfört till enheten för passagerarinformation innehåller andra än i 4 § 2 mom. nämnda passageraruppgifter, ska uppgifterna utplånas omedelbart efter det att de mottagits.

Passageraruppgifter från vilka de uppgifter som avses i 1 mom. har avskilts genom maskering får lämnas ut endast genom ett beslut av chefen för enheten för passagerarinformation eller av en av denne förordnad person som hör till personalen vid enheten för passagerarinformation. Om det är fråga om en begäran från en enhet för passagerarinformation i en annan medlemsstat krävs det dessutom att utlämnandet av uppgifterna rimligen kan antas vara behövligt för att terroristbrott och grov brottslighet ska kunna bekämpas.

12 §

Inskränkningar i rätten till insyn

Med avvikelse från 23 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten gäller rätten till insyn inte uppgifter om resultaten av behandlingen av passageraruppgifter.

Dataskyddsmyndigheten kan på begäran av en registrerad kontrollera att de uppgifter som avses i 1 mom. är lagenliga.

13 §

Personuppgiftsansvarig för passageraruppgifter

Polisstyrelsen är personuppgiftsansvarig för det register som innehåller passageraruppgifter.

14 §

Påföljdsavgift för lufttrafikföretag

Lufttrafikföretag som bryter mot skyldigheten i 4 § att överföra passageraruppgifter ska påföras en påföljdsavgift (påföljdsavgift för lufttrafikföretag). Avgiften är 3 000 euro för varje sådan flygning för vilken passageraruppgifter inte har överförts eller för vilken uppenbart bristfälliga uppgifter överförts.

Påföljdsavgift för lufttrafikföretag påförs inte om det vid överföringen av passageraruppgifterna har inträffat ett fel till följd av ouppmärksamhet som med beaktande av samtliga omständigheter är ursäktlig eller om det i övrigt med hänsyn till omständigheterna skulle vara oskäligt att påföra en avgift.

Påföljdsavgift för lufttrafikföretag får inte påföras den som är misstänkt för samma gärning i en förundersökning eller åtalsprövning eller i ett brottmål som är anhängigt vid en domstol. Påföljdsavgift för lufttrafikföretag får inte heller påföras den som genom en lagakraftvunnen dom har dömts till straff för samma gärning eller som för brott mot 20 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) har påförts påföljdsavgift för transportör enligt 179 § i utlänningslagen (301/2004).

15 §

Hörande av lufttrafikföretag

Innan en påföljdsavgift för transportör påförs ska lufttrafikföretaget ges tillfälle att skriftligen avge en förklaring inom en tid som inte får vara kortare än två veckor.

16 §

Påförande av påföljdsavgift för lufttrafikföretag

Påföljdsavgift för lufttrafikföretag påförs av en polisman som hör till befälet vid enheten för passagerarinformation. Påföljdsavgiften ska betalas till staten. Avgiften anges i beslutet. Ett beslut om påförande av påföljdsavgift ska iakttas även om ändring har sökts, om inte besvärsmyndigheten bestämmer något annat.

17 §

Betalningstid

Påföljdsavgiften för lufttrafikföretag ska betalas inom en månad från delfåendet av beslutet. På en påföljdsavgift som förfallit till betalning och som inte har betalats senast på förfallodagen tas en dröjsmålsränta ut enligt den räntesats som avses i 4 § 1 mom. i räntelagen (633/1982).

18 §

Verkställighet och ändringssökande

Verkställigheten av påföljdsavgiften för lufttrafikföretag sköts av rättsregistercentralen. Rättsregistercentralen ska underrättas om ett beslut av en myndighet eller domstol genom vilket påföljdsavgiften har sänkts eller avlyfts. Rättsregistercentralen ska utan ansökan betala tillbaka en påföljdsavgift som betalats utan grund.

En påföljdsavgift som påförts med stöd av denna lag verkställs i den ordning som föreskrivs i lagen om verkställighet av böter (672/2002).

Ett beslut om påföljdsavgift för lufttrafikföretag får överklagas genom besvär hos förvaltningsdomstolen på det sätt som föreskrivs i förvaltningsprocesslagen (586/1996). Förvaltningsdomstolens beslut får överklagas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

19 §

Ikraftträdande

Denna lag träder i kraft den 2018.

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder kraft.

3.

Lag

om ändring av 12 § i lagen om Enheten för utredning av grå ekonomi

I enlighet med riksdagens beslut

ändras i lagen om Enheten för utredning av grå ekonomi (1207/2010) 12 § 2 mom., sådant det lyder i lag 645/2015, som följer:

12 §

Behandling av personuppgifter och rätt till insyn

— —

En registrerad har dock inte rätt till insyn i de uppgifter som avses i 6 kap. 2 § 1 mom. i lagen om behandling av personuppgifter i polisens verksamhet (/) och i 42 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) och inte heller i uppgifter i de register som nämns i 29 § i lagen om behandling av personuppgifter inom Tullen (639/2015).

— —

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av 6 § i lagen om kontrollavgift i kollektivtrafik

I enlighet med riksdagens beslut

ändras i lagen om kontrollavgift i kollektivtrafik (469/1979) 6 § 5 mom., sådant det lyder i lagarna 761/2003 och 448/2006, som följer:

6 §

Biljettkontrollörer

— —

Polisen för en förteckning över beslut om godkännanden som kontrollör och återkallande av godkännanden. På behandlingen av personuppgifter tillämpas dessutom lagen om behandling av personuppgifter i polisens verksamhet (/).

———

Denna lag träder i kraft den 20 .

———

5.

Lag

om ändring av 15 § i lagen om besöksförbud

I enlighet med riksdagens beslut

ändras i lagen om besöksförbud (898/1998) 15 §, sådan den lyder i lag 711/2004, som följer:

15 §

Registrering av besöksförbud

På registrering och utplåning av uppgifter om besöksförbud tillämpas 2 kap. 5 § och 5 kap. 2 § i lagen om behandling av personuppgifter i polisens verksamhet (/).

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 17 § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

I enlighet med riksdagens beslut

ändras i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) 17 § 3 mom., sådant det lyder i lag 651/2015, som följer:

17 §

Teknisk övervakning

— —

På behandling av uppgifter som erhållits med hjälp av teknisk övervakningsutrustning tillämpas personuppgiftslagen (523/1999), lagen om behandling av personuppgifter i polisens verksamhet (/), gränsbevakningslagen (578/2005) eller lagen om behandling av personuppgifter inom Tullen (639/2015), oberoende av om upptagningarna utgör ett sådant personregister som avses i personuppgiftslagen eller inte.

———

Denna lag träder i kraft den 20 .

———

7.

Lag

om ändring av 9 § i lagen om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor

I enlighet med riksdagens beslut

ändras i lagen om tillämpning av Europaparlamentets och rådets förordning om ömsesidigt erkännande av skyddsåtgärder i civilrättsliga frågor (227/2015) 9 § som följer:

9 §

Registrering av skyddsåtgärder

Bestämmelser om registrering av uppgifter om i Finland verkställda skyddsåtgärder som har meddelats i en annan medlemsstat i Europeiska unionen i polisens informationssystem och om utplåning av uppgifter ur systemet finns i 8 kap. 3 § i lagen om behandling av personuppgifter i polisens verksamhet (/).

———

Denna lag träder i kraft den 20 .

———

8.

Lag

om ändring av 2 kap. 15 § i lagen om brottsbekämpning inom Tullen

I enlighet med riksdagens beslut

ändras i lagen om brottsbekämpning inom Tullen (623/2015) 2 kap. 15 § 2 mom., sådant det lyder i lag 310/2016, som följer:

2 kap.

Tullens befogenheter vid tullbrottsbekämpning

15 §

Identifiering

— —

Om någon vägrar lämna uppgifter enligt 1 mom. och om personen inte kan identifieras på annat sätt, har en tullman inom tullbrottsbekämpningen rätt att utreda identiteten med hjälp av signalement samt med stöd av de personregister som avses i lagen om behandling av personuppgifter inom Tullen (639/2015) och i 2 kap. 3 och 5 § i lagen om behandling av personuppgifter i polisens verksamhet (/). I sådana situationer ska det som föreskrivs i 8 kap. 33 § 2–4 mom. i tvångsmedelslagen om förrättande av genomsökning av personer iakttas.

— —

———

Denna lag träder i kraft den 20 .

———

9.

Lag

om ändring av 86 § i lagen om privata säkerhetstjänster

I enlighet med riksdagens beslut
ändras i lagen om privata säkerhetstjänster (1085/2015) 86 § som följer:

86 §

Uppgifter för tillsynen över säkerhetsbranschen

Polisen förvarar uppgifter om väktare, utbildare i användningen av maktmedel, skytteinstruktörer, ordningsvakter, utförare av säkerhetsskyddsuppgifter, utbildare av ordningsvakter, innehavare av näringstillstånd för säkerhetsbranschen och deras ansvariga föreståndare samt om i 71 § 2 mom. 2 punkten avsedda ansvariga personer (*uppgifter för tillsynen över säkerhetsbranschen*). På behandlingen av uppgifter för tillsynen över säkerhetsbranschen tillämpas lagen om behandling av personuppgifter i polisens verksamhet (/).

Denna lag träder i kraft den 20 .

10.

Lag

om ändring av 42 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten

I enlighet med riksdagens beslut

ändras i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014) 42 § 2 mom. som följer:

42 §

Rätt att få uppgifter ur vissa myndigheters register

— —

Bestämmelser om rätten att få uppgifter finns dessutom i lagen om behandling av personuppgifter i polisens verksamhet (/), lagen om behandling av personuppgifter vid verkställighet av straff (422/2002), lagen om försvarsmakten och någon annanstans i lag.

— —

———

Denna lag träder i kraft den 20 .

———

11.

Lag

om ändring av 17 § i lagen om behandling av personuppgifter inom Tullen

I enlighet med riksdagens beslut

ändras i lagen om behandling av personuppgifter inom Tullen (639/2015) 17 § 3 mom. som följer:

17 §

Utlämnande av uppgifter till andra myndigheter

— —

Trots vad som anges i 1 mom. 5 och 6 punkten får observationsuppgifter, uppgifter i underrättelseregistret enligt 4 § och uppgifter i temporära analysregister enligt 7 § 2 mom. inte användas för utförande av uppdrag enligt 2 kap. 11 § 1 mom. 7 punkten i lagen om behandling av personuppgifter i polisens verksamhet (/) och i 25 § 1 mom. 5 punkten i lagen om behandling av personuppgifter vid gränsbevakningsväsendet.

— —

———

Denna lag träder i kraft den 20 .

———————

12.

Lag

om ändring av 9 kap. 4 § och 10 kap. 62 § i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen (806/2011) 9 kap. 4 § 3 mom. och 10 kap. 62 § 1 mom. som följer:

9 kap.

Tvångsmedel i samband med särskilda undersökningsmetoder

4 §

Bestämning och registrering av DNA-profiler

— —

För utförande av uppgifter som anges i 1 § 1 mom. i polislagen (872/2011) får DNA-profiler registreras i polisens personregister. DNA-profiler som innehåller uppgifter om den registrerades andra personliga egenskaper än kön får dock inte registreras. Bestämmelser om utplåning av DNA-profiler ur registret finns i lagen om behandling av personuppgifter i polisens verksamhet (/).

10 kap.

Hemliga tvångsmedel

62 §

Begränsning av partsoffentlighet i vissa fall

En person vars rättigheter eller skyldigheter saken gäller har inte, oavsett 11 § i lagen om offentlighet i myndigheternas verksamhet (621/1999), rätt att få vetskap om användning av tvångsmedel enligt detta kapitel förrän en underrättelse enligt 60 § har gjorts. Han eller hon har inte heller rätt till insyn för registrerade enligt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

— —

———

Denna lag träder i kraft den 20 .

———

13.

Lag

om ändring av 113 § i skjutvapenlagen

I enlighet med riksdagens beslut

ändras i skjutvapenlagen (1/1998) 113 § 2 mom., sådant det lyder i lag 623/2017, som följer:

113 §

Polisens skyldighet att föra register

— —

De register som avses i 1 mom. är sekretessbelagda. Sekretessbelagda är också tillståndsansökningar som gäller skjutvapen, vapendelar, patroner eller särskilt farliga projektiler samt ansökningar om förhandssamtycke, samtycke och godkännande som vapensamlare samt beslut i en sådan sak. Polisen kan dock av särskilda skäl genom beslut bekräfta giltigheten för eller en uppgift i ett enskilt tillstånd, om identiteten för den som begär informationen är känd för polisen. På registerföringen samt användningen och utlämnandet av uppgifter ur registren tillämpas i övrigt lagen om behandling av personuppgifter i polisens verksamhet (/).

— —

———

Denna lag träder i kraft den 20 .

———

14.

Lag

om ändring av 42 b § i lotterilagen

I enlighet med riksdagens beslut

ändras i lotterilagen (1047/2001) 42 b § 2 mom., sådant det lyder i lag 1184/2013, som följer:

42 b §

Tillsynsregister över lotterier

— —

På behandlingen av personuppgifter i polisens register tillämpas lagen om behandling av personuppgifter i polisens verksamhet (/).

_____

Denna lag träder i kraft den 20 .

_____

15.

Lag

om ändring av 17 och 19 § i lagen om nödcentralsverksamhet

I enlighet med riksdagens beslut

upphävs i lagen om nödcentralsverksamhet (692/2010) 19 § 1 mom. 11 punkten, och

ändras 17 § 4 mom. och 19 § 1 mom. 1 och 11 punkten, sådana de lyder i lag 1172/2016, som följer:

17 §

Information som ska lagras i nödcentralsdatasystemet

— —

Bestämmelser om registrerades rätt att ta del av information som polisen lagrat i nödcentralsdatasystemet finns i 4 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) och i 6 kap. i lagen om behandling av personuppgifter i polisens verksamhet (/).

19 §

Rätt att få information ur registren

Nödcentralsverket och dess anställda har enligt vad som överenskommits med registerföraren och trots sekretessbestämmelserna, för att kunna sköta Nödcentralsverkets lagstadgade uppgifter, rätt att avgiftsfritt få information som behövs för att säkerställa förberedande åtgärder i samband med uppdrag eller arbetarskyddet eller för att stödja myndigheten eller enheten i fråga. I detta syfte har Nödcentralsverket och dess anställda rätt att

— —

1) få sådan information ur polisens informationssystem som avses i 2 kap. 3 och 5 § i lagen om behandling av personuppgifter i polisens verksamhet samt information ur det nationella system inom Schengens informationssystem som avses i 4 kap. 6 § i den lagen,

— —

11) få information ur tillfälliga personregister som har inrättats för polisens verksamhet, för sådana ändamål med behandlingen som avses i 2 kap. i lagen om behandling av personuppgifter i polisens verksamhet,

— —

———

Denna lag träder i kraft den 20 .

———

16.

Lag

om ändring av utlänningsregistret

I enlighet med riksdagens beslut

ändras i lagen om utlänningsregistret (1270/1997) 3 a § 2 mom., 3 b § 2 och 3 mom. och 4 a §, sådana de lyder, 3 a § 2 mom. i lag 459/2009 och 3 b § 2 och 3 mom. i lag 632/2011 samt 4 a § i lag 763/2003, som följer:

3 a §

Användning av fingeravtrycksuppgifter i delregistret för främlingspass och resedokument för flykting

— —

Rätt att använda uppgifterna har endast den som nödvändigtvis behöver dem för skötseln av sina arbetsuppgifter. Fingeravtryck får användas endast för fastställande av identitet och tillverkning av främlingspass eller resedokument för flykting. Polisen har dessutom rätt att använda fingeravtrycksuppgifter på det sätt som föreskrivs i 2 kap. 11 § 4 mom. i lagen om behandling av personuppgifter i polisens verksamhet (/). Den som har rätt att använda uppgifterna har rätt att ta fingeravtryck av en registrerad och jämföra dessa med registrerade fingeravtryck. Uppgifter som tagits för jämförelsen får användas endast när jämförelsen görs och ska därefter förstöras omedelbart.

3 b §

Användning och jämförelse av fingeravtrycksuppgifter i delregistret för ansökningsärenden

— —

Fingeravtryck som införs i registret får endast användas för att inom ramen för befogenheter i anknytning till de ändamål som anges i 2 § 2 mom. verifiera autenticiteten av ett uppehållstillståndskort och identiteten hos innehavaren av ett uppehållstillstånd, för behandling, beslut och övervakning av utlänningars inresa och utresa samt vistelse och arbete och för tryggande av statens säkerhet. En myndighet som har rätt att använda uppgifterna har rätt att jämföra dem med tidigare registrerade fingeravtryck i delregistret för ansökningsärenden och med fingeravtrycksuppgifter i delregistret för främlingspass och resedokument för flykting och med fingeravtryck som med stöd av 131 § i utlänningslagen registrerats i polisens register. Dessutom får uppgifter för kontroll av inreseförutsättningarna jämföras med fingeravtryck som ingår i signalementsuppgifterna enligt tvångsmedelslagen och som avses i 2 kap. 2 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet, när de redan registrerade fingeravtrycksuppgifterna har samband med ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst ett år.

Polisen har dessutom rätt att använda de fingeravtrycksuppgifter som registrerats i delregistret för ansökningsärenden på det sätt som föreskrivs i 2 kap. 11 § 4 mom. i lagen om behandling av personuppgifter i polisens verksamhet.

— —

4 a §

Den registrerades rättigheter

I fråga om den registrerades rätt till uppgifter som polisen förvarar i utlänningsregistret enligt 2 § gäller vad som föreskrivs i 4 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) och i 6 kap. i lagen om behandling av personuppgifter i polisens verksamhet.

Denna lag träder i kraft den 20 .

17.

Lag

om ändring av 131 § i utlänningslagen

I enlighet med riksdagens beslut

ändras i utlänningslagen (301/2004) 131 § 2 och 3 mom., sådana de lyder i lag 631/2011, som följer:

131 §

Upptagande av signalement

— —

De i 1 mom. avsedda signalementen införs i ett register som polisen för. Uppgifterna ska hållas åtskilda från signalementen för personer som är misstänkta för brott och från de fingeravtryck som i enlighet med 3 b § i lagen om utlänningsregistret (1270/1997) införs i utlänningsregistret och som tas för ansökan om uppehållstillstånd, uppehållstillståndskort eller uppehållskort för unionsmedborgares familjemedlemmar. Uppgifterna avförs i enlighet med 5 kap. 2 § i lagen om behandling av personuppgifter i polisens verksamhet (/).

Fingeravtrycksuppgifter som avses i 1 mom. får jämföras med fingeravtrycksuppgifter som har registrerats med stöd av denna paragraf och som avses i 2 kap. 2 § 3 mom. i lagen om behandling av personuppgifter i polisens verksamhet samt med fingeravtrycksuppgifter som registrerats i delregistret för ansökningsärenden och delregistret för främlingspass och resedokument för flykting, vilka ingår i det utlänningsregister som nämns i 3 § i lagen om utlänningsregistret. Dessutom får fingeravtrycksuppgifter som införs för kontroll av inreseförutsättningarna jämföras med fingeravtryck som ingår i signalementsuppgifterna enligt tvångsmedelslagen och som avses i 2 kap. 2 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet, när de redan registrerade fingeravtrycksuppgifterna har samband med ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst ett år.

— —

———

Denna lag träder i kraft den 20 .

———

18.

Lag

om ändring av 27 § i lagen om penninginsamlingar

I enlighet med riksdagens beslut
ändras i lagen om penninginsamlingar (255/2006) 27 § 2 mom. som följer:

27 §

Tillsynsregister över penninginsamlingar

— —

På behandlingen av personuppgifter i polisens register tillämpas lagen om behandling av personuppgifter i polisens verksamhet (/).

_____

Denna lag träder i kraft den 20 .

_____

19.

Lag

om ändring av 29 § i passlagen

I enlighet med riksdagens beslut

ändras i passlagen (671/2006) 29 § 1 och 2 mom., sådana de lyder i lag 456/2009, som följer:

29 §

Passregister

För utförande av de uppgifter som enligt denna lag ankommer på polisen, utrikesministeriet och en sådan finsk beskickning som avses i 10 § ska polisen föra ett register där det förs in

1) de behövliga grundläggande personuppgifter som avses i 2 kap. 1 § i lagen om behandling av personuppgifter i polisens verksamhet (/),

2) uppgifter om passansökningar och beslut i passärenden, uppgifter om pass och andra resehandlingar som har utfärdats av en finsk myndighet, uppgifter om pass som har förkommit, blivit stulna eller tillvaratagits samt uppgifter om hinder för utfärdande av pass och anmärkningar som hänför sig till passärenden,

3) fingeravtryck som enligt 6 a § tagits av sökanden vid ansökan om pass; fingeravtryck som registrerats i fingeravtrycksuppgifterna får med den berörda personens samtycke även användas för utarbetande av en identitetshandling som personen ansökt om senare,

4) ett fotografi av personen och personens namnteckningsprov, som personen lämnat till polisen, utrikesministeriet eller till en myndighet inom utrikesförvaltningen vid ansökan om pass; med personens samtycke får personens fotografi och namnteckningsprov även användas för utarbetande av något annat förvaltningstillstånd eller beslut som personen ansökt om än för den handling som fotografiet och namnteckningsprovet har lämnats för.

I fråga om användning av uppgifter i passregistret gäller vad som föreskrivs i 2 kap. 9 och 11 § i lagen om behandling av personuppgifter i polisens verksamhet. I fråga om utlämnande och utplåning av uppgifter i passregistret gäller vad som föreskrivs i 4 kap. och 5 kap. 4 § i den lagen. I fråga om skyddet av sådana identifieringsuppgifter som grundar sig på en persons fysiska egenskaper gäller vad som föreskrivs i 8 kap. 1 § i nämnda lag.

———————————————————————————————————————

———

Denna lag träder i kraft den 20 .

———————

20.

Lag

om ändring av 17 och 31 § i lagen om identitetskort

I enlighet med riksdagens beslut
ändras i lagen om identitetskort (663/2016) 17 § 5 mom. och 31 § som följer:

17 §

Förvägrande av identitetskort och identitetskort utan rätt att resa

— —

Uppgift om utfärdande av ett sådant identitetskort som avses i 3 mom. antecknas i polisens personregister.

31 §

Identitetskortsregister

För utförande av de uppgifter som enligt denna lag ankommer på polisen och finska beskickningar ska polisen föra ett register där det förs in

1) de behövliga grundläggande personuppgifter som avses i 2 kap. 1 § i lagen om behandling av personuppgifter i polisens verksamhet (/),

2) uppgifter om i denna lag avsedda ansökningar, beslut, tillstånd, polisens och finska beskickningars åtgärder, hinder, anmärkningar och anmälningar,

3) ett fotografi av personen och personens namnteckningsprov, som personen lämnat till polisen, utrikesministeriet eller till en myndighet inom utrikesförvaltningen vid ansökan om identitetskort; med personens samtycke får personens fotografi och namnteckningsprov även användas för utarbetande av något annat förvaltningstillstånd eller beslut som personen ansökt om än för den handling som fotografiet och namnteckningsprovet har lämnats för.

Bestämmelser om användningen av uppgifterna i registret finns i 2 kap. 9 och 11 § i lagen om behandling av personuppgifter i polisens verksamhet. Bestämmelser om utlämnande och utplåning av uppgifter finns i 4 kap. och 5 kap. 4 § i den lagen.

———

Denna lag träder i kraft den 20 .

———————

21.

Lag

om ändring av lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet

I enlighet med riksdagens beslut

ändras i lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rådets rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009) 3 §, 5 § 2 och 3 mom. samt 6 § 2 och 3 mom.,

sådana de lyder, 3 § i lag 1180/2013, 5 § 2 mom. och 6 § 2 mom. i lag 312/2016 samt 5 § 3 mom. och 6 § 3 mom. i lag 649/2015, som följer:

3 §

Definition av information och underrättelser

I denna lag avses med information och underrättelser

1) uppgifter som avses i 2 kap. i lagen om behandling av personuppgifter i polisens verksamhet (/),

2) uppgifter i Tullens personregister enligt 2 kap. i lagen om behandling av personuppgifter inom Tullen (639/2015),

3) uppgifter i de personregister som avses i 3, 4 och 7–12 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005), samt

4) uppgifter som annars med stöd av 4 kap. 2 och 3 § samt 5 kap. 40–42 § i polislagen (872/2011), 3 kap. 1 § i lagen om behandling av personuppgifter i polisens verksamhet, 2 kap. 14 § i lagen om brottsbekämpning inom Tullen (623/2015), 17, 18 och 22 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet eller någon annan lag eller ett avtal innehas av polisen, Tullen eller gränsbevakningsväsendet eller som är tillgängliga för dem utan att de vidtar tvångsåtgärder.

5 §

Utlämnande av information och underrättelser på begäran

— —

Information och underrättelser lämnas ut under de förutsättningar som anges i 4 kap. 5 § i lagen om behandling av personuppgifter i polisens verksamhet, 17 § i lagen om behandling av personuppgifter inom Tullen och 26–28 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet.

På beslutsfattande som gäller utlämnande av information och underrättelser tillämpas vad som föreskrivs i 4 kap. i lagen om behandling av personuppgifter i polisens verksamhet, 18 § i lagen om behandling av personuppgifter inom Tullen, 29 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet samt någon annanstans i lag.

6 §

Utlämnande av information och underrättelser på eget initiativ

— —

Information och underrättelser lämnas ut under de förutsättningar som anges i 4 kap. 5 § i lagen om behandling av personuppgifter i polisens verksamhet, 17 § i lagen om behandling av personuppgifter inom Tullen och 26–28 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet.

På beslutsfattande som gäller utlämnande av information och underrättelser tillämpas vad som föreskrivs i 4 kap. i lagen om behandling av personuppgifter i polisens verksamhet, 18 § i lagen om behandling av personuppgifter inom Tullen, 29 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet samt någon annanstans i lag.

Denna lag träder i kraft den 20 .

22.

Lag

om ändring av lagen om genomförande av vissa bestämmelser i beslutet om Eurojust

I enlighet med riksdagens beslut

ändras i lagen om genomförande av vissa bestämmelser i beslutet om Eurojust (742/2010) 10 § 2 mom., sådant det lyder i lag 648/2015, som följer:

10 §

Utlämnande av personuppgifter till Eurojust

— —

Vid utlämnande av uppgifter till Eurojust ur polisens, gränsbevakningsväsendets och Tullens personregister tillämpas 4 kap. 5 § i lagen om behandling av personuppgifter i polisens verksamhet (/), 38 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005), 26 § i lagen om behandling av personuppgifter inom Tullen (639/2015) och 30 § i lagen om offentlighet i myndigheternas verksamhet (621/1999).

— —

———

Denna lag träder i kraft den 20 .

———

23.

Lag

om ändring av 1 och 19 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut

ändras i lagen om verkställighet av böter (672/2002) 19 § 2 mom. och

fogas till 1 § 1 mom., sådant det lyder i lagarna 224/2008, 462/2011, 348/2013, 257/2014, 671/2015, 451/2016 och 470/2017, en ny 12 punkt som följer:

1 §

Lagens tillämpningsområde

I den ordning som föreskrivs i denna lag verkställs följande påföljder:

— —

12) påföljdsavgift för lufttrafikföretag enligt 14 § i lagen om genomförande av direktivet om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

— —

19 §

Efterlysning

— —

Efterlysningen omfattar en uppmaning som riktar sig till polismännen och som har införts i polisens informationssystem. Enligt uppmaningen ska en polisman när den betalningsskyldige påträffas driva in en fordran som avses i 1 mom. eller stämma in den betalningsskyldige till en rättegång för bestämmande av förvandlingsstraff. Efterlysningen ska innehålla de uppgifter som behövs för betalning av fordran och redovisning av prestationen samt förvaringstiden för registeruppgifterna.

— —

———

Denna lag träder i kraft den 20 .

———

24.

Lag

om ändring av 7 b § i lagen om stark autentisering och betrodda elektroniska tjänster

I enlighet med riksdagens beslut

ändras i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 7 b §, sådan den lyder i lag 533/2016, som följer:

7 b §

Information om giltighet för pass eller identitetskort

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att med hjälp av teknisk anslutning få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering

———

Denna lag träder i kraft den 20 .

———

25.

Lag

om ändring av 5 kap. 41 och 60 § i polislagen

I enlighet med riksdagens beslut
ändras i polislagen (872/2011) 5 kap. 41 § 1 mom. och 60 § 1 mom. som följer:

5 kap.

Hemliga metoder för inhämtande av information

41 §

Behandling av uppgifter om en informationskälla och betalning av arvode

Uppgifter om en informationskälla får registreras i ett personregister. På behandlingen av uppgifterna tillämpas lagen om behandling av personuppgifter i polisens verksamhet (/).
— —

60 §

Begränsning av partsoffentlighet i vissa fall

En person vars rättigheter eller skyldigheter saken gäller har inte, oavsett 11 § i lagen om offentlighet i myndigheternas verksamhet (621/1999), rätt att få vetskap om användningen av en metod för inhämtande av information enligt detta kapitel förrän en underrättelse enligt 58 § har gjorts. Han eller hon har inte heller rätt till insyn för registrerade enligt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).
— —

———

Denna lag träder i kraft den 20 .

———

26.

Lag

om ändring av 5 § i lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning

I enlighet med riksdagens beslut

ändras i lagen om Europeiska unionens byrå för samarbete inom brottsbekämpning (214/2017) 5 § som följer:

5 §

Nationell tillsynsmyndighet

Dataskyddsmyndigheten är i Finland den nationella tillsynsmyndighet som avses i artikel 42.1 i Europolförordningen.

Denna lag träder i kraft den 20 .

27.

Lag

om ändring av lagen om behandlingen av personer i förvar hos polisen

I enlighet med riksdagens beslut

ändras i lagen om behandlingen av personer i förvar hos polisen (841/2006) 1 kap. 7 § 5 mom., 2 kap. 4 § 2 mom., 7 kap. 1 § 2 mom. och 5 § 5 mom. samt 12 kap. 2 § 3 mom., av dem 1 kap 7 § 5 mom. sådant det lyder i lag 1086/2015, som följer:

1 kap.

Allmänna bestämmelser

7 §

Ställningen för en väktare som är anställd av en innehavare av näringstillstånd inom säkerhetsbranschen

— —

En väktare som avses i denna paragraf har inte användarrättigheter till polisens personregister, på vilka tillämpas lagen om behandling av personuppgifter i polisens verksamhet (/) och inte heller till andra register eller informationssystem som har upprättats för myndighetsändamål.

2 kap.

Intagning i förvaringslokal

4 §

Ankomstgranskning och registrering av uppgifter

— —

Bestämmelser om registrering av uppgifter om frihetsberövade som intagits i en förvaringslokal finns i lagen om behandling av personuppgifter i polisens verksamhet.

7 kap.

Besök och andra kontakter utanför förvaringslokalen

1 §

Besök

— —

Besök hos den frihetsberövade ska övervakas på behövligt sätt. Besök kan även övervakas med videoutrustning. Den frihetsberövade och besökaren ska på lämpligt sätt underrättas om övervakning med videoutrustning. På förvaring och utplåning av upptagningar som uppkom-

mit vid övervakningen tillämpas 2 kap. 10 § och 5 kap. 2 och 3 § i lagen om behandling av personuppgifter i polisens verksamhet.

— —

5 §

Besöksförbud

— —

På behandlingen av uppgifter om besöksförbud i polisens personregister tillämpas lagen om behandling av personuppgifter i polisens verksamhet.

— —

12 kap.

Teknisk övervakning

2 §

Upptagning

— —

På förvaring och utplåning av upptagningar som uppkommit vid teknisk övervakning tillämpas 2 kap. 10 § samt 5 kap. 2 och 3 § i lagen om behandling av personuppgifter i polisens verksamhet.

— —

———

Denna lag träder i kraft den 20 .

———

28.

Lag

om ändring av 5 och 6 § i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet

I enlighet med riksdagens beslut

ändras i lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009) 5 § 1 mom. och 6 § 1 mom., sådana de lyder, 5 § 1 mom. i lag 881/2011 och 6 § 1 mom. i lag 642/2015, som följer:

5 §

PTG-kriminalunderrättelseenheter

För PTG-myndigheternas kriminalunderrättelse- och brottsanalysverksamhet finns en riksomfattande PTG-underrättelseenhet, utöver vilken det kan inrättas regionala och lokala PTG-kriminalunderrättelseenheter. En PTG-kriminalunderrättelseenhet kan bestå av företrädare för PTG-myndigheterna som förordnas särskilt och även av företrädare för andra myndigheter.

6 §

Behandlingen av uppgifter vid PTG- kriminalunderrättelseenheterna

I fråga om behandlingen av personuppgifter vid en PTG-kriminalunderrättelseenhet gäller vad som föreskrivs i lagen om behandling av personuppgifter i polisens verksamhet (/), lagen om behandling av personuppgifter vid gränsbevakningsväsendet (/) och lagen om behandling av personuppgifter inom Tullen (/).

Denna lag träder i kraft den 20 .

29.

Lag

om ändring av säkerhetsutredningslagen

I enlighet med riksdagens beslut

ändras i säkerhetsutredningslagen (726/2014) 25 § 1 mom. 4 punkten och 2 mom., 32 § 1 mom. 2 punkten och 3 mom., 49 och 56 § samt 61 § 2 mom. som följer:

25 §

Informationskällor vid normal säkerhetsutredning av person

En säkerhetsutredning av person får bygga enbart på registeruppgifter som finns i

— —

4) polisens personregister som innehåller sådana uppgifter som avses i 2 kap. 3, 5 och 9 § samt 7 kap. i lagen om behandling av personuppgifter i polisens verksamhet (/).

— —

För en normal säkerhetsutredning får användas en anmälan som centralkriminalpolisen gjort utifrån sådana uppgifter om persongrupper i polisens personregister som avses i 2 kap. 4 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet. Anmälan ska innehålla sådana uppgifter som skyddspolisen behöver för att bedöma informationens betydelse. Centralkriminalpolisen får göra en anmälan, ifall

1) den som utredningen gäller utifrån de uppgifter som avses i 2 kap. 4 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet har återkommande kontakter av permanent natur med sådana personer som enligt domstolsbeslut ansetts ha deltagit i en organiserad kriminell sammanslutnings verksamhet eller som i en pågående förundersökning eller åtalsprövning misstänkts ha deltagit i sådan verksamhet, om kontakterna kan göra den som utredningen gäller mottaglig för extern osaklig påverkan och därmed riskera skyddet för ett intresse som ligger till grund för säkerhetsutredningen, eller

2) centralkriminalpolisen utifrån de uppgifter som avses i 2 kap. 4 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet och andra eventuella upplysningar anser att det föreligger grundad anledning att misstänka att den som utredningen gäller gjort sig skyldig till deltagande i en organiserad kriminell sammanslutnings verksamhet och det är nödvändigt att förmedla informationen för att skydda ett intresse som ligger till grund för säkerhetsutredningen mot åtgärder eller påverkan från organiserade kriminella sammanslutningars sida eller för att förebygga brott, eller

3) det i de uppgifter som avses i 2 kap. 4 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet i fråga om den som utredningen gäller finns flera sådana anteckningar som till sin natur och sitt innehåll är betydande för bedömningen av personens tillförlitlighet och som sammantagna ger centralkriminalpolisen grundad anledning att misstänka att den som utredningen gäller kan äventyra skyddet för de handlingar på skyddsnivåerna I och II och uppgifterna i dem som personen fått i den arbetsuppgift som ligger till grund för utredningen och därmed gynna organiserade kriminella sammanslutningars åtgärder, om det är nödvändigt att förmedla informationen för att skydda statens viktiga säkerhetsintressen mot åtgärder eller påverkan från organiserade kriminella sammanslutningars sida eller för att förebygga brott.

— —

32 §

Begränsning av användningen av uppgifter i säkerhetsutredning av person

Vid en säkerhetsutredning av person får följande uppgifter inte användas:

— —

2) personuppgifter i anknytning till sådan kriminalunderrättelseinhämtning som avses i 2 kap. 4 § i lagen om behandling av personuppgifter i polisens verksamhet och sådana observationsuppgifter som avses i 2 kap. 6 § i den lagen,

— —

Sådana uppgifter om en persons hälsotillstånd som ingår i de uppgifter som avses i 2 kap. 3, 5 och 9 § samt i 7 kap. i lagen om behandling av personuppgifter i polisens verksamhet, får beaktas när en utredning görs endast om det är nödvändigt för att trygga andras personliga säkerhet och uppgifterna baserar sig på ett läkarintyg eller andra anteckningar av en legitimerad yrkesutbildad person inom hälso- och sjukvården eller på uppgifter som han eller hon lämnat muntligt med stöd av lag, och det inte råder oklarhet om att uppgifterna är korrekta. Vad som föreskrivs ovan i detta moment hindrar inte den behöriga myndigheten från att fästa arbetsgivarens uppmärksamhet på behovet att vidta i 17 § 2 mom. 4 punkten avsedda åtgärder.

49 §

Avförande av uppgifter ur registret över säkerhetsutredningar

De uppgifter som förts in i registret över säkerhetsutredningar ska avföras senast tre år efter det att en ny motsvarande säkerhetsutredning har gjorts eller giltigheten för en säkerhetsutredning eller ett intyg över säkerhetsutredning har upphört eller de arbetsuppgifter för vilka säkerhetsutredningen gjordes har upphört eller intyget över säkerhetsutredning har återkallats. På avförande av uppgifter tillämpas i övrigt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

56 §

Dataskyddsmyndighetens rätt att utöva tillsyn

Dataskyddsmyndigheten har rätt att ta del av en säkerhetsutredning som har gjorts med stöd av denna lag för att kontrollera att behandlingen av personuppgifter är laglig.

Bestämmelser om dataskyddsmyndighetens rätt att utöva tillsyn över och få information om behandlingen av personuppgifter finns i 8 kap. i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

61 §

Hänvisning till straffbestämmelser

— —

Bestämmelser om straff för dataskyddsbrott finns i 38 kap. 9 § i strafflagen.

———

Denna lag träder i kraft den 20 .

———

30.

Lag

om ändring av 3 och 4 § i lagen om centralen för utredning av penningvätt

I enlighet med riksdagens beslut

ändras i lagen om centralen för utredning av penningvätt (445/2017) 3 § 6, 8 och 9 mom. samt 4 § 4 mom. som följer:

3 §

Registret för förhindrande, avslöjande och utredning av penningtvätt och av finansiering av terrorism

— —

De registrerade har inte rätt till annan insyn i registret än till uppgifter i anslutning till de frysningsbeslut som avses i 2 § 1 mom. 7 punkten. Dataskyddsmyndigheten kan på begäran av en registrerad kontrollera att behandlingen av uppgifterna om den registrerade är lagenlig.

— —

Logguppgifter och övervakningsuppgifter om databehandling enligt 5 § 4 mom. ska på begäran tillställas dataskyddsmyndigheten för påseende. Logguppgifter ska bevaras endast i syfte att säkerställa skyddet för personuppgifter och för att trygga datasäkerheten och rättssäkerheten, och de ska skyddas mot osaklig hantering. Logguppgifter och övervakningsuppgifter ska bevaras i tio år.

— —

Bestämmelser om polisens behandling av personuppgifter finns dessutom i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) och i lagen om behandling av personuppgifter i polisens verksamhet (/).

4 §

Centralens rätt att få, använda och lämna ut uppgifter

— —

De uppgifter som centralen erhållit får oberoende av sekretessbestämmelserna användas och lämnas ut endast för att förhindra, avslöja och utreda penningtvätt, finansiering av terrorism och det brott genom vilket den egendom eller den vinning har fåtts eller kan fås som är föremål för penningtvätt eller finansiering av terrorism samt för att föra ärendet till undersökning. Centralen för utredning av penningtvätt kan lämna ut uppgifter också utan begäran. Dessutom får uppgifter lämnas ut till utrikesministeriet för skötsel av uppgifter enligt 9 § i lagen om frysning av tillgångar i syfte att bekämpa terrorism och till utmätningsmannen för skötsel av uppgifter enligt 14 § i den lagen och uppgifter enligt 2 b § i lagen om uppfyllande av vissa förpliktelser som grundar sig på Finlands medlemskap i Förenta Nationerna och Europeiska unionen (659/1967). Uppgifter kan lämnas ut också till en behörig tillsynsmyndighet som avses i lagen om förhindrande av penningtvätt och av finansiering av terrorism, om den uppgift som lämnas ut är nödvändig för att den behöriga tillsynsmyndigheten ska kunna utföra de uppgifter som avses i denna lag. Sådant beslut om utlämnande av uppgifter som avses i detta moment fattas av en polisman som hör till befälet och arbetar vid centralen för utredning av penningtvätt. Uppgifter som avses i detta moment får lämnas ut som en datamängd eller i elektronisk form.

— —

Denna lag träder i kraft den _____ 20 _____ .

31.

Lag

om ändring av lagen om förhindrande av penningtvätt och av finansiering av terrorism

I enlighet med riksdagens beslut

ändras i lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017) 4 kap. 3 § 2 mom. och 4 § 3 mom. samt 7 kap. 8 § 3 mom. och 9 § 3 mom. som följer:

4 kap.

Rapporteringsskyldighet, tystnadsplikt och avbrytande av transaktioner

3 §

Bevarande av uppgifter om tvivelaktiga affärstransaktioner

— —

De registrerade har inte rätt till insyn i de uppgifter som avses i 1 mom. eller de uppgifter och handlingar som inhämtats för fullgörande av utredningsskyldigheten enligt 3 kap. 4 § 3 mom. Dataskyddsmyndigheten kan på begäran av en registrerad kontrollera att behandlingen av uppgifterna är lagenlig.

4 §

Tystnadsplikt och undantag från tystnadsplikten i fråga om tvivelaktiga affärstransaktioner

— —

Trots tystnadsplikten enligt 1 mom. får en rapporteringsskyldig informera om rapportering enligt 1 § till sådana rapporteringsskyldiga som avses i 1 kap. 2 § 1 mom. 1 och 2 punkten och som har fått koncession i Finland eller i en annan EES-stat, när de medverkar i en enskild transaktion som hänför sig till den kund och den transaktion som rapporten avser. Informationen får också under samma förutsättningar lämnas ut till en rapporteringsskyldig enligt 1 kap. 2 § 1 mom. 1 eller 2 punkten som har beviljats koncession i någon annan stat än en EES-stat, om mottagaren av informationen har skyldigheter som motsvarar skyldigheterna enligt denna lag och fullgörandet av skyldigheterna övervakas och mottagaren dessutom har sådana skyldigheter i fråga om skydd för personuppgifter som motsvarar Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

— —

7 kap.

Tillsyn

8 §

Förfarande vid rapportering av misstänkta överträdelser hos en rapporteringsskyldig

— —

En registrerad person som en rapport avser har inte rätt till insyn i information som avses i 1 och 2 mom., om utlämnande av informationen skulle kunna försvåra utredningen av brott eller missbruk. Dataskyddsmyndigheten kan på begäran av en registrerad person granska att de uppgifter om den registrerade som avses i 1 och 2 mom. är lagenliga.

9 §

System för mottagande av rapport om misstanke om överträdelser

— —

En registrerad person som en rapport avser har inte rätt till insyn i information som avses i 1 och 2 mom., om utlämnande av informationen skulle kunna försvåra utredningen av brott eller missbruk. Dataskyddsmyndigheten kan på begäran av en registrerad granska att de uppgifter om den registrerade som avses i 1 och 2 mom. är lagenliga.

———

Denna lag träder i kraft den 20 .

———

32.

Lag

om ändring av 49 § i lagen om Polisyrkeshögskolan

I enlighet med riksdagens beslut
ändras i lagen om Polisyrkeshögskolan (1164/2013) 49 § 1 mom. som följer:

49 §

Hantering av känslig information

I ärenden som gäller antagning av studerande, disciplin, avbrytande av studierna och indragning av studierätten har Polisyrkeshögskolan rätt att hantera personuppgifter som rör hälsotillstånd och domar i brottmål och överträdelser. I samband med ett disciplinärende får dock inte uppgifter som gäller den studerandes hälsotillstånd hanteras.

———

Denna lag träder i kraft den 20 .

———

33.

Lag

om ändring av 13 § i lagen om vittnesskyddsprogram

I enlighet med riksdagens beslut
ändras i lagen om vittnesskyddsprogram (88/2015) 13 § 1 och 3 mom. som följer:

13 §

Register över vittnesskyddsprogram

Centralkriminalpolisen ska för skötseln av sina uppgifter enligt denna lag föra ett register över vittnesskyddsprogram. I registret ska också ingå upptagningar och andra handlingar som uppstått i verksamheten. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av i registret införda personuppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999) samt på annan behandling av personuppgifter lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

— —

Utöver vad som föreskrivs i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten kan den registrerades rätt till insyn begränsas, om utövandet av rätten till insyn på sannolika skäl kan leda till ett allvarligt hot mot den skyddades eller någon annans säkerhet.

———

Denna lag träder i kraft den 20 .

———