Regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till vissa lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Genom lagen genomförs det nya dataskyddsdirektivet.

Den föreslagna lagen ska tillämpas på behandling av personuppgifter som utförs av polisen, åklagarna, de allmänna domstolarna, Brottspåföljdsmyndigheten, Tullen, Gränsbevakningsväsendet och andra behöriga myndigheter, när det är fråga om förebyggande, avslöjande och utredning av brott eller förande av brott till åtalsprövning, åklagarverksamhet i samband med brott, handläggning av brottmål i domstol, verkställighet av straffrättsliga påföljder eller skydd mot eller förhindrande av brott mot den allmänna säkerheten. Lagen ska också tillämpas när Försvarsmakten, polisen och Gränsbevakningsväsendet behandlar personuppgifter i samband med upprätthållande av den nationella säkerheten. Det är till denna del fråga om en nationell lösning.

I ovannämnda situationer ska den föreslagna lagen tillämpas som allmän lag. Avvikelser från lagens bestämmelser kan göras i speciallagstiftning.

Den föreslagna lagen ska innehålla bestämmelser om ändamålsbegränsning och andra allmänna principer för behandling av personuppgifter, den personuppgiftsansvariges och personuppgiftsbiträdets ansvar, rätten till insyn och andra rättigheter för den registrerade, krav på informationssäkerhet, utnämning av ett dataskyddsombud och dataskyddsombudets uppgifter, krav när personuppgifter överförs till tredjeländer, tillsynen över efterlevnaden av lagen samt rättsmedel och påföljder.

Tillsynen över efterlevnaden av lagen ska utövas av dataombudsmannen.

I samband med den föreslagna lagen föreslås det ändringar också i straffregisterlagen, lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen, lagen om justitieförvaltningens riksomfattande informationssystem, lagen om verkställighet av böter och lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten.

Propositionen hänför sig till den första tilläggsbudgetpropositionen för 2018, men avses inte bli behandlad i samband med den.

Lagarna avses träda i kraft den 6 maj 2018 eller så snart som möjligt efter det.

INNEHÅLL

ALLMÄN MOTIVERING

1 Inledning

Syftet med denna proposition är att genomföra Europaparlamentets och rådets direktiv 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 *det nya dataskyddsdirektivet, dataskyddsdirektivet* eller *direktivet*). Direktivet trädde i kraft den 5 maj 2016 och ska genomföras senast den 6 maj 2018.

Samtidigt med dataskyddsdirektivet antog Europaparlamentet och rådet också förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*allmän dataskyddsförordning*). Direktivet och förordningen bildar tillsammans det s.k. dataskyddspaketet, som syftar till att reformera den gällande dataskyddslagstiftningen inom EU. Allmänna dataskyddsförordningen är som sådan tillämplig rätt i medlemsstaterna och ska börja tillämpas den 25 maj 2018. Avsikten är att allmänna dataskyddsförordningen i Finland ska kompletteras genom nationell lagstiftning, som har beretts separat (RP 19/2018 rd).

Den gällande dataskyddslagstiftningen inom EU består av ett direktiv som antogs 1995 (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, nedan *dataskyddsdirektivet från 1995*) och av ett rambeslut från 1995 om straffrättsligt samarbete och polissamarbete i samband med brottmål (Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, nedan *rambeslutet*).

Syftet med dataskyddspaketet är att uppdatera och modernisera de principer som ingick i det tidigare dataskyddsdirektivet och i rambeslutet, särskilt med beaktande av den snabba informationstekniska utvecklingen samt den ständigt växande behandlingen av personuppgifter. Reformen har som särskilt innehållsmässigt mål att förbättra de registrerades rättigheter, stärka den inre marknaden inom EU, säkerställa en hög nivå på skyddet för personuppgifter när brottmål handläggs och även annars i samhället, säkerställa att dataskyddsbestämmelserna iakttas och övervakas samt främja personuppgifters rörlighet.

Dataskyddsdirektivet från 1995 genomfördes i Finland huvudsakligen genom personuppgiftslagen (523/1999). Utöver den innehåller gällande lagstiftning väldigt mycket specialbestämmelser om dataskydd. Bestämmelserna i dataskyddsdirektivet är klart mer detaljerade än den gällande nationella allmänna lagstiftningen och skiljer sig delvis från den. Avsikten är dessutom att upphäva personuppgiftslagen genom nationell lagstiftning som kompletterar allmänna dataskyddsförordningen. Av nämnda skäl föreslås det att en ny lag om behandling av personuppgifter i brottmål ska stiftas.

Varken dataskyddsdirektivet eller allmänna dataskyddsförordningen blir på grund av sina tillämpningsbestämmelser tillämpliga på sådan behandling av personuppgifter som utförs i samband med verksamhet som ligger utanför unionsrättens tillämpningsområde. De tillämpas bl.a. inte på behandling av personuppgifter som sker i samband med tryggandet av den nationella säkerheten. För att behandlingen av personuppgifter ska bli reglerad på ett heltäckande sätt i Finland, ska den föreslagna lagen tillämpas också när Försvarsmakten, polisen och Gränsbevakningsväsendet behandlar personuppgifter i samband med upprätthållande av den nationella säkerheten.

2 Det nya dataskyddsdirektivet

2.1 Allmänt

Europeiska kommissionen lämnade sitt förslag till allmän dataskyddsförordning och till dataskyddsdirektiv den 27 januari 2012. Kommissionens initiativ baserade sig på omfattande samrådsmöten och konsekvensbedömningar som ägde rum under 2009—2011. Förslaget till direktiv och förslaget till förordning behandlades samtidigt i rådet.

Syftet med dataskyddsdirektivet är att säkerställa skyddet för personuppgifter på direktivets tillämpningsområde samt underlätta det fria flödet av uppgifter mellan polismyndigheter och straffrättsliga myndigheter i medlemsstaterna. Det är delvis till sin karaktär ett s.k. minimidirektiv, eftersom det inte hindrar medlemsstaterna från att införa bestämmelser om en högre skyddsnivå för den registrerades rättigheter.

Rådets rambeslut 2008/977/RIF om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete upphävs genom dataskyddsdirektivet från och med den 6 maj 2018. Båda rättsakterna strävar efter att säkerställa en enhetlig och hög skyddsnivå för fysiska personer vid behandlingen av personuppgifter i brottmål och underlätta utbytet av personuppgifter mellan behöriga myndigheter i medlemsstaterna. Rambeslutet, som upphävs, gäller dock endast behandlingen av sådana personuppgifter som överförs mellan medlemsstaterna, medan dataskyddsdirektivet också gäller behandling av personuppgifter inom en medlemsstat. Dessutom är dataskyddsdirektivet mer detaljerat och har ett bredare tillämpningsområde än dataskyddsrambeslutet, och innehåller färre möjligheter till undantag än rambeslutet.

2.2 Det huvudsakliga innehållet i dataskyddsdirektivet

Direktivets struktur

Direktivet innehåller nio kapitel. Kapitlen tar upp allmänna bestämmelser, principer, den registrerades rättigheter, personuppgiftsansvarig och personuppgiftsbiträde, överföringar av personuppgifter till tredjeländer eller internationella organisationer, oberoende tillsynsmyndigheter, samarbete, rättsmedel, ansvar och sanktioner, genomförandeakter samt slutbestämmelser.

Allmänna bestämmelser

Direktivets tillämpningsområde definieras i artikel 2. Direktivet ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Direktivet ska tillämpas också när det är fråga om att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Direktivet ska dock inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av unionens institutioner, organ och byråer. Utanför tillämpningsområdet faller således verksamheten inom bl.a. Europol och Eurojust samt nationell säkerhet och nationellt försvar. Trots begränsningen av tillämpningsområdet gör direktivet det möjligt att på nationell nivå utsträcka de i direktivet angivna bestämmelserna till behandling av personuppgifter inom området nationell säkerhet och nationellt försvar.

I artikel 3 definieras bl.a. begreppen personuppgifter, behandling, behörig myndighet, personuppgiftsansvarig, mottagare och internationell organisation. Med personuppgifter avses varje

upplysning som avser en identifierad eller identifierbar enskild person (*en registrerad*). Med behörig myndighet avses en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Begreppet behörig myndighet utsträcks i definitionen till att gälla också andra organ eller enheter som genom lag har anförtrotts myndighetsutövning eller getts befogenheter i något syfte som nämns ovan.

Principer

Artiklarna 4—11 i direktivet innehåller bestämmelser om de allmänna principerna för behandling av personuppgifter.

Medlemsstaterna ska enligt artikel 4 bl.a. föreskriva att personuppgifter ska behandlas på ett lagligt sätt och att de ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål än det ursprungliga ska dock tillåtas förutsatt att det föreskrivs om behandlingen i lag och den är nödvändig och står i proportion till detta andra ändamål. Artikel 4.3 innehåller specialbestämmelser om behandling för arkivändamål samt vetenskaplig, statistisk eller historisk användning. Kravet på att behandlingen ska vara laglig preciseras i artikel 8, enligt vilken behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet inom direktivets tillämpningsområde och som sker på grundval av lag.

Enligt vad som föreskrivs i artikel 6 ska det i tillämpliga fall och så långt det är möjligt göras en klar åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom personer som dömts för brott och brottsoffer. Även personuppgifter som grundar sig på fakta ska så lång det är möjligt åtskiljas från personuppgifter som grundar sig på personliga bedömningar (artikel 7).

Artikel 10 innehåller bestämmelser om behandling av särskilda kategorier av personuppgifter. Med särskilda kategorier av personuppgifter avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom även genetiska uppgifter, biometriska uppgifter samt uppgifter om hälsa eller sexuell läggning eller sexualliv. Artikel 11 innehåller bestämmelser om profilering, inbegripet förbud mot att använda sådan profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter. Direktivet förutsätter också att datasäkerheten och kvaliteten på uppgifterna säkerställs.

De registrerades rättigheter

Artiklarna 12—18 innehåller bestämmelser om vilka lagstiftningsåtgärder som krävs av medlemsstaterna för att trygga de registrerades rättigheter.

Enligt artikel 13 ska den personuppgiftsansvarige göra bl.a. följande information tillgänglig för den registrerade: den personuppgiftsansvariges identitet, ändamålen med den behandling för vilken personuppgifterna är avsedda, uppgifter om dataskyddsombudet, om ett sådant finns, liksom även information om rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

Enligt artikel 14 ska den registrerade ha rätt att av den personuppgiftsansvarige få bekräftelse av huruvida personuppgifter som rör honom eller henne håller på att behandlas. Den registrerade ska också ha rätt att få tillgång till personuppgifterna och få information bl.a. om ändamålen med behandlingen och dess rättsliga grund. Enligt artikel 16 ska den registrerade ha rätt

att kräva att den personuppgiftsansvarige rättar felaktiga personuppgifter som rör den registrerade. Direktivet gör det möjligt för den registrerade att utöva sina rättigheter genom dataskyddsmyndigheten.

Medlemsstaterna kan dock föreskriva om rätt att begränsa tillhandahållandet av ovannämnda uppgifter eller skyldigheten att rätta personuppgifter, om en sådan åtgärd är nödvändig för att undvika att hindra officiella förfaranden, för att trygga förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet att straffrättsliga påföljder, för att skydda den allmänna säkerheten, för att skydda den nationella säkerheten eller för att skydda andra personers rättigheter och friheter (artikel 13.3, artikel 15, artikel 16.4).

Enligt artikel 18 får medlemsstaterna föreskriva om de registrerades rätt till insyn och rättelse i sin nationella lagstiftning, om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden. Enligt skäl 16 i ingressen i direktivet påverkar direktivet inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar.

Personuppgiftsansvarig och personuppgiftsbiträde

I artiklarna 19—34 föreskrivs det om den personuppgiftsansvariges och personuppgiftsbiträdets ansvar, säkerhet för personuppgifter och dataskyddsombudet.

Enligt artikel 19 ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa, och kunna visa, att behandlingen utförs i enlighet med direktivet. Sådana åtgärder ska vidtas i synnerhet för att säkerställa att nödvändiga skyddsåtgärder integreras i behandlingen (s.k. inbyggt dataskydd, artikel 20.1) och att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas (s.k. dataskydd som standard, artikel 20.2).

Artikel 21 innehåller bestämmelser om den inbördes ansvarsfördelningen i de fall då minst två personuppgiftsansvariga gemensamt fastställer behandlingens ändamål och medel. De betraktas då som gemensamt personuppgiftsansvariga.

Om behandlingen av personuppgifter läggs ut, får den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra ovannämnda tekniska och organisatoriska åtgärder (artikel 22.1). Den personuppgiftsansvarige och personuppgiftsbiträdet ska upprätta ett avtal eller någon annan rättsakt där bl.a. föremålet för behandlingen, behandlingens varaktighet, art och ändamål anges (artikel 22.3).

Den personuppgiftsansvarige och personuppgiftsbiträdet ska föra ett register över verksamheter i samband med behandling som de ansvarar för. Närmare bestämmelser om innehållet i registret har tagits in i artikel 24.

De loggar som avses i artikel 25 ska föras i automatiserade behandlingssystem. Loggar ska föras över följande typer av behandlingar: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna. Loggarna får endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet samt inom ramen för straffrättsliga förfaranden.

Artikel 27 innehåller bestämmelser om den personuppgiftsansvariges skyldighet att utföra en konsekvensbedömning avseende dataskydd. En bedömning ska utföras om en typ av behandling, med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Om det är fråga om ett nytt register som ska inrättas och en konsekvensbedömning visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, ska tillsynsmyndigheten höras innan behandlingen av personuppgifterna inleds (artikel 28). Tillsynsmyndigheten ska höras också om typen av behandling medför en hög risk för de registrerades rättigheter och friheter, t.ex. vid användning av ny teknik eller nya rutiner eller förfaranden.

Artikel 29 innehåller bestämmelser om den personuppgiftsansvariges och personuppgiftsbiträdets skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå. När det gäller automatiserad behandling ska de t.ex. vidta åtgärder i syfte att vägra varje obehörig person åtkomst till utrustning som används för behandling, förhindra obehörig läsning samt säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet.

Den personuppgiftsansvarige ska vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, anmäla den till tillsynsmyndigheten (artikel 30). Personuppgiftsbiträdet är för sin del skyldigt att underrätta den personuppgiftsansvarige om personuppgiftsincidenter.

Den personuppgiftsansvarige ska informera också den registrerade om personuppgiftsincidenten om den sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter. Under vissa förutsättningar behöver den registrerade inte informeras, bl.a. om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att ovannämnda risker sannolikt inte kommer att uppstå. Informationen till den registrerade kan senareläggas, begränsas eller utelämnas, om en sådan åtgärd är nödvändig för att undvika att hindra officiella förfaranden, för att trygga förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet att straffrättsliga påföljder, för att skydda den allmänna säkerheten, för att skydda den nationella säkerheten eller för att skydda andra personers rättigheter och friheter.

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Medlemsstaterna får undanta domstolars och andra oberoende rättsliga myndigheters dömande verksamhet från denna skyldighet. Bestämmelser om utnämning av dataskyddsombudet, dataskyddsombudets ställning och dataskyddsombudets uppgifter finns i artiklarna 32—34.

Överföringar av personuppgifter till tredjeländer eller internationella organisationer

I artiklarna 35—38 finns det bestämmelser om vilka villkor som ska uppfyllas för att personuppgifter ska kunna överföras till tredjeländer eller internationella organisationer. Överföringen ska för det första vara nödvändig när behöriga myndigheter i tredjelandet sköter uppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Uppgifter kan överföras endast till ett sådant tredjeland för vilket Europeiska kommissionen har antagit ett beslut om adekvat skyddsnivå. Om kommissionen inte har antagit ett sådant beslut för landet i fråga, får uppgifterna överföras förutsatt att åtgärder för skydd av personuppgifterna har fastställts i ett avtal eller att den personuppgiftsansvarige har gjort en omfattande bedömning och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger. Om det inte finns något beslut av kommissionen eller lämpliga skyddsåtgärder saknas, får personuppgifter överföras endast av ytterst vägande skäl, t.ex. för att skydda intres-

sen som är av grundläggande betydelse för en fysisk person eller för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i ett land.

Oberoende tillsynsmyndigheter

Varje medlemsstat ska ha minst en oberoende myndighet med ansvar att övervaka de i direktivet angivna rättigheterna i landet i fråga. Denna tillsynsmyndighet kan vara samma myndighet som övervakar efterlevnaden av den allmänna dataskyddsförordningen i landet i fråga (artiklarna 41 och 45). Varje tillsynsmyndighet ska vara oberoende (artikel 42). I dess behörighet ingår dock inte att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet.

Enligt artikel 46 behandlar och undersöker tillsynsmyndigheten klagomål som gäller iakttagande av de rättigheter som anges i direktivet. Utöver sin tillsynsuppgift har den oberoende myndigheten omfattande uppgifter som handlar om att öka medvetenheten, ge rådgivning, avge yttranden och idka samarbete (artiklarna 46—50). Utförandet av tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och för dataskyddsombudet. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den upprepas, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Tillsynsmyndigheten ska ha effektiva befogenheter att få tillgång till information och andra befogenheter (artikel 47).

Samarbete

I artikel 50 har det tagits in bestämmelser om att tillsynsmyndigheterna i medlemsstaterna är skyldiga att samarbeta med varandra. I artikeln föreskrivs det bl.a. om det förfarande som ska följas vid samarbete i tillsynsärenden. I artikel 51 i direktivet föreskrivs det om den genom den allmänna dataskyddsförordningen inrättade dataskyddsstyrelsens uppgifter på direktivets tillämpningsområde. Styrelsen ska utfärda rekommendationer om tillämpningen av direktivet samt avge ett yttrande till kommissionen huruvida skyddsnivån i ett tredjeland är adekvat.

Rättsmedel, ansvar och sanktioner

Enligt artikel 52 ska alla registrerade personer ha rätt att lämna in ett klagomål till tillsynsmyndigheten, om de anser att behandling som avser dem står i strid med de bestämmelser som antas i enlighet med direktivet. Den registrerade ska underrättas av den behöriga tillsynsmyndigheten om klagomålets handläggning och dess resultat. Enligt artikel 53 ska en fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och som meddelats av en tillsynsmyndighet, utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol. Varje registrerad person ska ha rätt till ett effektivt rättsmedel, om tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller om tillsynsmyndigheten inte informerar den registrerade om handläggningen eller resultatet av klagomålet.

Medlemsstaterna ska dessutom i enlighet med artikel 54 föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med lag. Enligt artikel 55 ska medlemsstaterna i enlighet med sin nationella processrätt se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte vars mål är av allmänt intresse och som är verksam för att främja skyddet av personuppgifter, i uppdrag att lämna in klagomålet för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

Den registrerade ska ha rätt till ersättning för materiell eller immateriell skada till följd av en åtgärd som står i strid med de bestämmelser som antas i enlighet med direktivet (artikel 56). Medlemsstaterna ska föreskriva sanktioner för överträdelser av bestämmelser som antas enligt direktivet och ska vidta de åtgärder som krävs för att säkerställa att dessa sanktioner genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande (artikel 57).

Genomförandeakter och slutbestämmelser

Enligt artikel 59 upphävs rådets rambeslut 2008/977/RIF genom direktivet. Enligt artikel 63 ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa direktivet. De ska genast överlämna texten till dessa bestämmelser till kommissionen och tillämpa dem från och med den 6 maj 2018. Medlemsstaterna får dock föreskriva att de automatiserade behandlingssystem som inrättades före den 6 maj 2016, när det innebär oproportionella ansträngningar, ska bringas i överensstämmelse med artikel 25 senast den 6 maj 2023. Om fullgörandet av skyldigheten att föra loggar under exceptionella omständigheter skulle medföra allvarliga problem för driften av det automatiserade behandlingssystemet, kan övergångsperioden förlängas till högst den 6 maj 2026.

Enligt artikel 60 ska direktivet inte påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter som trädde i kraft den 6 maj 2016 eller tidigare.

Enligt artikel 61 ska avtal som innehåller bestämmelser om överföring av personuppgifter och som medlemsstaterna ingått med tredjeländer eller internationella organisationer före ikraftträdandet av direktivet, fortsätta att gälla tills de ändras eller återkallas, dock under förutsättning att dessa avtal är förenliga med unionsrätten så som den tillämpades innan direktivet antogs.

3 Nuläge

3.1 Nationell lagstiftning och praxis

Allmänt

Enligt 10 § 1 mom. i grundlagen utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Allmänna lagar som gäller myndigheternas behandling av personuppgifter i brottmål är personuppgiftslagen (523/1999) och lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan *offentlighetslagen*).

I Finland har dataskyddsdirektivet från 1995 genomförts genom personuppgiftslagen och senare ändringar av den samt genom bestämmelserna i 16 § 3 mom. i offentlighetslagen. Bestämmelser som genomför dataskyddsdirektivet från 1995 ingår också i lagen om datasekretessnämnden och dataombudsmannen (389/1994), i förordningen om datasekretessnämnden och dataombudsmannen (432/1994) och i 38 kap. 1, 2, 8 och 9 § samt 40 kap. 5 § i strafflagen (39/1889).

Personuppgiftslagen är en allmän lag och har ett mer omfattande tillämpningsområde än dataskyddsdirektivet från 1995. Personuppgiftslagen tillämpas också på behandling av personuppgifter som sker på dataskyddsrambeslutets tillämpningsområde, om inte något annat föreskrivs någon annanstans i lag.

Med behandling av personuppgifter avses i personuppgiftslagen alla åtgärder som vidtas i fråga om personuppgifterna, såsom insamling, registrering, organisering, användning, översändande, utlämnande, lagring, ändring, samkörning, blockering, utplåning och förstöring av

personuppgifter. Personuppgiftslagen tillämpas på automatisk behandling av personuppgifter samt på annan behandling då personuppgifterna utgör eller är avsedda att utgöra ett personregister eller en del av ett sådant. Personuppgiftslagen innehåller bestämmelser om de allmänna principerna för behandlingen av personuppgifter, behandling av känsliga uppgifter och personbeteckning, behandling av personuppgifter för särskilda ändamål, såsom forskning, översändande av personuppgifter till ett tredjeland, datasäkerhet, styrning och övervakning av behandlingen av personuppgifter samt påföljder.

På förande av personregister och behandlingen av personuppgifter hos myndigheter tillämpas dessutom flera särskilda författningar.

Lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) innehåller bestämmelser om ett riksomfattande informationssystem som betjänar behandlingen och verkställigheten av rättskipningsärenden. I lagen föreskrivs det om registrering, utlämnande och annan behandling av uppgifter om ärenden som är anhängiga hos domstolarna, åklagarmyndigheterna och rättshjälpsmyndigheterna och om ärenden som har avgjorts av dem. Domstolarna, åklagarmyndigheterna och rättshjälpsbyråerna är skyldiga att ansluta sig och överföra uppgifter till informationssystemet. Rättsregistercentralen är registeransvarig för justitieförvaltningens riksomfattande informationssystem. De uppgifter som registrerats i informationssystemet är sekretessbelagda, och får därmed inte lämnas ut, om inte något annat särskilt föreskrivs i lag. Utanför lagens tillämpningsområde faller informationssystem hos enskilda myndigheter.

Enligt straffregisterlagen (770/1993) inhämtas till, registreras i och lämnas ur straffregistret uppgifter som behövs för bestämmande och verkställighet av straffrättsliga påföljder. Rättsregistercentralen är registeransvarig för straffregistret. De uppgifter som registrerats i straffregistret ska hemlighållas, och får därmed inte lämnas ut, om inte något annat särskilt föreskrivs i lag. Lagen innehåller bestämmelser också om utplåning av uppgifter ur straffregistret.

Lagen om verkställighet av böter (672/2002) innehåller bestämmelser om förande av ett bötesregister. Rättsregistercentralen är registeransvarig för bötesregistret. Bötesregistret förs och används för verkställighet av ärenden som ska verkställas i den ordning som föreskrivs i lagen om verkställighet av böter. Uppgifterna i bötesregistret om brott och straffrättsliga påföljder ska hållas hemliga. De uppgifterna få lämnas ut endast till dem vilkas rätt att få uppgifterna regleras särskilt genom lag. Lagen innehåller också bestämmelser om utplåning av uppgifter ur bötesregistret.

Lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012, nedan *EU-straffregisterlagen*) innehåller bestämmelser om överföring av uppgifter ur straffregistret och bötesregistret till den medlemsstat i Europeiska unionen där den dömda personen är medborgare samt om lagring i Finland av sådana registeruppgifter om finska medborgare som har överförts till Finland från en annan medlemsstat. Utlämnande av uppgifter ur straffregistret och bötesregistret till den medlemsstat där den dömda personen är medborgare sker i enlighet med 5 § i EU-straffregisterlagen. I fråga om utlämnande av straffregisteruppgifter till ett annat nordiskt land gäller dessutom vad som föreskrivs genom förordning.

Rättsregistercentralen för med stöd av EU-straffregisterlagen ett lagringsregister i syfte att lagra sådana uppgifter om finska medborgare som har överförts till Finland så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag. De uppgifter som har antecknats i lagringsregistret är sekretessbelagda. Rådets rambeslut 2009/315/RIF om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll har genomförts genom EU-straffregisterlagen. Genom de reg-

ler som fastställts i rambeslutet kompletteras de befintliga allmänna reglerna för skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Det informationsutbyte som anges i rambeslutet sker via centralmyndigheterna i medlemsstaterna. Centralmyndighet i Finland är Rättsregistercentralen.

Lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten (1069/2015) innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Lagen gäller verkställighet av bötesstraff endast i fråga om förvandlingsstraff för böter. I fråga om villkorligt fängelsestraff gäller lagen endast övervakning som dömts ut som tilläggsstraff till villkorligt fängelse som ålagts unga, eftersom ett villkorligt fängelsestraff som dömts ut utan övervakning inte kräver verkställighetsåtgärder. Lagen gäller även den verkställighet av häktning som Brottspåföljdsmyndigheten utför samt Brottspåföljdsmyndighetens åtgärder och den behandling av personuppgifter som krävs i dem för utredning i fråga om förutsättningarna för utdömande av påföljd eller beredning av verkställighet av en påföljd. Till Brottspåföljdsmyndighetens riksomfattande personregister hör verkställighetsregistret, samhällspåföljdsregistret, övervaknings- och verksamhetsregistret, säkerhetsregistret och besökarregistret.

I utsökningsbalken (705/2007) föreskrivs det om utsökningens informationssystem, vilket är ett för skötseln av utsökningsmyndigheternas uppgifter inrättat informationssystem som är avsett för utsökningsmyndigheternas riksomfattande bruk och som drivs med hjälp av automatisk databehandling. Riksfogdeämbetet sörjer för driften och utvecklandet av informationssystemet. Till utsökningens informationssystem hör ett utsökningsregister, som består av en riksomfattande indexdel och registerdelar som förs lokalt. Utsökningsregistret förs av de lokala utsökningsmyndigheterna tillsammans. Riksfogdeämbetet sörjer för den allmänna driften av registret och meddelar föreskrifter om hur uppgifterna tekniskt ska föras in och behandlas. På behandlingen av personuppgifter som har samlats in för utsökningsregistret och som har förts in i det tillämpas personuppgiftslagen, om inte något annat föreskrivs i utsökningsbalken. Utsökningsbalken innehåller bestämmelser bl.a. om de registrerades rätt till insyn, avförande av uppgifter ur utsökningsregistret och utlämnande av uppgifter myndigheter emellan. En del av de uppgifter som införts i utsökningsregistret är sekretessbelagda.

De uppgifter om brottmål som avses i det nya dataskyddsdirektivet utlämnas från andra EU-medlemsstater till finska myndigheter för ett enskilt ärende med tillämpning av bestämmelserna om internationellt straffrättsligt samarbete. Det internationella straffrättsliga samarbetet omfattar bl.a. inbördes rättshjälp i brottmål, utlämning för brott samt samarbete för överföring av verkställighet av fängelsestraff och andra straffrättsliga påföljder.

Den viktigaste rättsakten om internationell straffrättslig hjälp mellan medlemsstaterna i Europeiska unionen är rådets direktiv 2014/41/EU om en europeisk utredningsorder på det straffrättsliga området. Det har i Finland genomförts genom lagen om genomförande av direktivet om en europeisk utredningsorder på det straffrättsliga området (430/2017). Lagen trädde i kraft den 3 juni 2017.

I förhållande till de medlemsstater på vilka direktivet om en utredningsorder inte är tillämpligt, tillämpas de bestämmelser som gällde tidigare. De bestämmelserna tillämpas också när det är fråga om sådan straffrättslig hjälp på vilket direktivet inte tillämpas. De viktigaste multilaterala fördragen om inbördes straffrättslig hjälp är europeiska konventionen om inbördes rättshjälp i brottmål (FördrS 30/1981) och konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (FördrS 56/2004), som ingicks 2000. Bestämmelser om internationell rättshjälp i brottmål finns dessutom i lagen om internationell rättshjälp i straffrättsliga ärenden (4/1994).

Utlämning för brott mellan Europeiska unionens medlemsstater sker utgående från rådets rambeslut 2002/584/RIF om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna. Rambeslutet har i Finland genomförts genom lagen om utlämning för brott mellan Finland och de övriga medlemsstaterna i Europeiska unionen (1286/2003). Bestämmelser om utlämning för brott till Europeiska unionens medlemsstater finns också i lagen om utlämning för brott mellan Finland och de övriga nordiska länderna (1383/2007).

Överföring av dömda mellan Europeiska unionens medlemsstater sker utgående från rådets rambeslut 2008/909/RIF. Rambeslutet har genomförts nationellt genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rambeslutet om överföring av dömda personer inom Europeiska unionen och om tillämpning av rambeslutet (1169/2011).

Det samarbete inom EU som gäller verkställighet av bötesstraff och erkännande av beslut om förverkande baserar sig på rambesluten 2005/214/RIF och 2006/783/RIF, vilka har genomförts genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rambeslutet om tillämpning av principen om ömsesidigt erkännande på bötesstraff och om tillämpning av rambeslutet (231/2007) och genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rambeslutet om tillämpning av principen om ömsesidigt erkännande på beslut om förverkande och om tillämpning av rambeslutet (222/2008).

Det samarbete som gäller frysning baserar sig på rådets rambeslut 2003/577/RIF, som har genomförts nationellt genom lagen om verkställighet i Europeiska unionen av frysningsbeslut av egendom eller bevismaterial (540/2005).

Samarbetet mellan medlemsstaterna regleras också i rådets rambeslut 2008/947/RIF, som har genomförts genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rambeslutet om alternativa påföljder och övervakningsåtgärder inom Europeiska unionen och om tillämpning av rambeslutet (1170/2011). Rådets rambeslut 2009/829/RIF har genomförts genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i rambeslutet om övervakningsåtgärder som ett alternativ till tillfälligt frihetsberövande och om tillämpning av rambeslutet (620/2012). Rådets rambeslut 2009/948/RIF har genomförts genom lagen om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden och om överföring av förundersökning och lagföring mellan Finland och de övriga medlemsstaterna i Europeiska unionen (295/2012). Rådets direktiv 2011/99/EU om den europeiska skyddsordern har genomförts genom lagen om det nationella genomförandet av de bestämmelser som hör till området för lagstiftningen i Europaparlamentets och rådets direktiv om den europeiska skyddsordern och om tillämpning av direktivet (226/2015).

Det samarbete som gäller utbyte att straffregisteruppgifter mellan medlemsstaterna i Europeiska unionen baserar sig på rådets rambeslut 2009/315/RIF, som har genomförts genom lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012).

Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (*Passenger Name Record*, PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (nedan *direktivet om passageraruppgifter*) antogs den 27 april 2016. Genomförandet av det har ännu inte slutförts. En del av genomförandebestämmelserna i direktivet om passageraruppgifter ska gälla behandling av personuppgifter, på vilken den lag som föreslås i denna proposition ska tillämpas som komplement.

Lagstiftning om behandling av personuppgifter i polisens verksamhet

På behandlingen av personuppgifter hos polisen tillämpas som speciallag lagen om behandling av personuppgifter i polisens verksamhet (761/2003, *polisens personuppgiftslag*). Där föreskrivs det om informationssystemet för polisärenden, informationssystemet för misstänkta och Skyddspolisens funktionella informationssystem. Lagen innehåller också bestämmelser bl.a. om användning och utlämnande av uppgifter, utplåning och arkivering av uppgifter samt behandling av personuppgifter i samband med internationellt polissamarbete. Utöver ovannämnda informationssystem finns det i flera speciallagar som gäller polisverksamhet bestämmelser om enskilda personregister hos polisen eller om en skyldighet att upprätthålla register som innehåller personuppgifter. Sådana personregister är t.ex. det penningtvättsregister som avses i lagen om centralen för utredning av penningtvätt (445/2017), det register över vittnesskyddsprogram som avses i lagen om vittnesskyddsprogram (88/2015), det passregister som avses i passlagen (671/2006) samt de register för skötsel av tillstånds- och tillsynsuppgifter som avses i skjutvapenlagen (1/1998). Dessutom innehåller lagen om samarbete mellan polisen, Tullen och gränsbevakningsväsendet (687/2009, nedan PTG-lagen) bestämmelser om behandling av uppgifter i ett tillfälligt register för brottsanalys, som var och en av dessa samarbetande myndigheter kan inrätta med stöd av sin egen lagstiftning om behandling av personuppgifter. En del av polisens personregister kommer att falla under dataskyddsförordningens tillämpningsområde och en del under den föreslagna lagens tillämpningsområde.

Bestämmelser som gäller behandling av personuppgifter i polisens verksamhet ingår också i vissa EU-rättsakter och lagar för genomförande av dem, vilka tillämpas på polissamarbetet mellan medlemsstaterna i samband med de uppgifter som avses i tillämpningsbestämmelsen i det nya dataskyddsdirektivet. Sådana rättsakter är i synnerhet 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, Europaparlamentets och rådets förordning (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 (Eurodac-förordningen), rådets beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet och rådets beslut 2008/616/RIF om genomförande av beslut 2008/615/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 de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater och om tillämpning av rambeslutet (26/2009).

Lagstiftning om behandling av personuppgifter inom Försvarsmakten

För närvarande finns det ingen koncentrerad lagstiftning om behandling av personuppgifter som skulle gälla försvarsförvaltningen, utan bestämmelser om detta finns utspridda på flera olika lagar. Speciallagstiftning om behandling av personuppgifter finns i värnpliktslagen

(1438/2007), lagen om försvarsmakten (551/2007), lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014), territorialövervakningslagen (755/2000) och lagen om militär krishantering (211/2006). Dessutom innehåller lagen om frivilligt försvar (556/2007) bestämmelser om Försvarsutbildningsföreningens behandling av personuppgifter. Bestämmelserna gäller främst Försvarsmaktens permanenta personregister, de uppgifter som införs i dem, rättigheter att få och lämna ut uppgifter samt vissa registervisa begränsningar i den registrerades rättigheter. Till övriga delar tillämpas bestämmelserna i personuppgiftslagen på den behandling av personuppgifter som Försvarsmakten utför.

Lagstiftning om behandling av personuppgifter inom Tullen

Lagen om behandling av personuppgifter inom Tullen (639/2015, nedan *Tullens personuppgiftslag*) innehåller bestämmelser om personregister och behandling av personuppgifter inom Tullen. Permanenta personregister vid Tullen är informationssystemet för brottsbekämpning, underrättelseregistret, informationssystemet för tullövervakning och systemet för identifiering av registreringsskyltar och containrar.

Lagens tillämpningsområde omfattar automatisk behandling av personuppgifter som behövs för skötseln av de uppdrag som i lag föreskrivs för Tullen och annan behandling av personuppgifter, då de utgör eller är avsedda att utgöra ett personregister eller en del av ett sådant. Utgångspunkten för Tullens personuppgiftslag är att avvikelse från den gällande personuppgiftslagen och offentlighetslagen görs endast om det är nödvändigt för att trygga en effektiv tullverksamhet eller för att beakta bestämmelser som gäller Europeiska unionens tull- eller andra informationssystem. Avvikelse från nämnda lagar görs närmast i fråga om bestämmelser som gäller insamling och registrering av känsliga uppgifter, den registrerades rätt till insyn och användning och utlämnande av personuppgifter. Lagen innehåller också bestämmelser om inrättande av personregister, datainnehållet i Tullens personregister, behandling av uppgifter, registeransvarig, hur länge uppgifterna i personregistren bevaras, nationellt och internationellt informationsutbyte samt tillsyn över användningen av registren. I syfte att effektivisera myndighetssamarbetet och informationsutbytet i samband med brottsbekämpning har Tullens personuppgiftslag utformats så att bestämmelserna så långt det är möjligt överensstämmer med bestämmelserna i polisens personuppgiftslag. De mest betydande skillnaderna beror på att dessa myndigheter har olika slags uppgifter, informationssystem och register. En del av Tullens personregister kommer att falla under dataskyddsförordningens tillämpningsområde och en del under den föreslagna lagens tillämpningsområde. Vid Tullen tillämpas dessutom vissa av ovannämnda EU-rättsakter som även tillämpas på polisens verksamhet och lagarna för genomförande av dem när det gäller samarbetet mellan tillsynsmyndigheterna på tillämpningsområdet för dataskyddsdirektivet.

Lagstiftning om behandling av personuppgifter vid Gränsbevakningsväsendet

På behandlingen av personuppgifter vid Gränsbevakningsväsendet tillämpas som speciallag lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005, *Gränsbevakningsväsendets personuppgiftslag*). Där föreskrivs det om Gränsbevakningsväsendets permanenta riksomfattande personregister. De är undersöknings- och handräckningsregistret, registret för tillståndsärenden, registret för övervakningsärenden, Gränsbevakningsväsendets register över personer misstänkta för brott, säkerhetsdataregistret, registret för militärrättsvården och registret för disciplinavgöranden. Lagen innehåller också bestämmelser om inrättande av andra riksomfattande eller regionala personregister, användning, utlämnande, utplåning och arkivering av personuppgifter samt behandling av personuppgifter i samband med internationellt samarbete. Bestämmelser om behandling av personuppgifter i sjöräddningstjänsten och om sjöräddningsregistret finns i sjöräddningslagen (1145/2001) och om värnpliktsregistret i värnpliktslagen (1438/2007). Inom Gränsbevakningsväsendet tillämpas dessutom vissa av

ovannämnda EU-rättsakter som även tillämpas på polisens verksamhet och lagarna för genomförande av dem när det gäller samarbetet mellan tillsynsmyndigheterna på tillämpningsområdet för dataskyddsdirektivet.

3.2 Internationella förpliktelser

EU-lagstiftning

Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (nedan *EUF-fördraget*) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Enligt artikel 8 i stadgan ska dessa uppgifter behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Dataskyddsdirektivet från 1995 syftade till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna. Dataskyddsdirektivet från 1995 tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg liksom på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Det tillämpas inte på polissamarbete och rättsligt samarbete i brottmål.

Rådets dataskyddsrambeslut 2008/977/RIF gäller behandling av sådana personuppgifter i brottmål som överförs eller görs tillgängliga mellan medlemsstaterna. Innan dataskyddsrambeslutet antogs fanns det i EU inga enhetliga dataskyddsbestämmelser om polissamarbete och straffrättsligt samarbete, även om specialbestämmelser har ingått t.ex. i Eurojust-beslutet från 2002. Dataskyddsrambeslutet skiljer sig från dataskyddsdirektivet bl.a. i fråga om sitt tillämpningsområde, eftersom det endast gäller utbyte av personuppgifter mellan behöriga myndigheter i medlemsstaterna. Rambeslutet innehåller också mer handlingsutrymme nationellt än dataskyddsdirektivet.

Internationella fördrag

Skyddet av personuppgifter är begreppsmässigt nära kopplat till skyddet för privatlivet. Skyddet för privatlivet är en central rättighet som tryggas i flera internationella konventioner om mänskliga rättigheter. Rätten till skydd för privatlivet berörs bl.a. av artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (FördrS 19/1990), artikel 17 i FN:s konvention om medborgerliga och politiska rättigheter (FördrS 7—8/1976) samt artikel 16 i FN:s konvention om barnets rättigheter (FördrS 59—60/1991).

Något som på ett betydande sätt inverkat på lagstiftningen om skydd av personuppgifter i Europa är Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (FördrS 35—36/1992, nedan *dataskyddskonventionen*). Europarådet antog dataskyddskonventionen 1981. Den har fungerat som underlag också för dataskyddsdirektivet från 1995.

Konventionen var det första rättsligt bindande internationella instrumentet på dataskyddsområdet. Bestämmelserna i konventionen erbjuder ett minimiskydd vid behandling av personuppgifter för alla personer som vistas på de staters territorier som ratificerat konventionen samt vid gränsöverskridande överföring av personuppgifter. Den ålägger de fördragsslutande parterna att i sin nationella lagstiftning föreskriva om åtgärder för att säkerställa att individens rättigheter respekteras vid behandlingen av personuppgifter. Dataskyddskonventionen tilläm-

pas på automatisk behandling av personuppgifter och gäller all behandling av personuppgifter, inklusive behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete. Med stöd av konventionen har det också utfärdats en mängd rekommendationer om behandling av personuppgifter.

Konventionen har ratificerats av 47 medlemsstater i Europarådet och av tre stater utanför Europarådet. Alla medlemsstater i EU är avtalsslutande parter. I Finland trädde konventionen i kraft år 1992. Dataskyddskonventionen kompletterades 2001 med ett tilläggsprotokoll om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181). Tilläggsprotokollet har ratificerats av 36 medlemsstater i Europarådet, inklusive Finland. Dessutom har tilläggsprotokollet ratificerats av tre stater utanför Europarådet. Tilläggsprotokollet trädde i kraft för Finlands del 2012.

Inom Europarådet har det utarbetats ett utkast till tilläggsprotokoll för att anpassa konventionen till nuvarande och kommande dataskyddsutmaningar. Förhandlingarna som saken pågår.

Lagstiftningen i utlandet

Den personuppgiftslagstiftning som ska tillämpas i samband med behandling av brottmål är för närvarande förhållandevis oenhetlig i EU-staterna. Detta beror bl.a. på att dataskyddsdirektivet från 1995 inte gäller sådan behandling. Inte heller genomförandet av dataskyddsrambeslutet har lett till någon betydande tillnärmning mellan medlemsstaternas nationella lagstiftning, vilket beror på begränsningar i rambeslutets tillämpningsområde samt det handlingsutrymme som det ger medlemsstaterna.

Eftersom lagstiftningen i Europeiska unionens medlemsstater som bäst undergår stora förändringar på grund av det nationella genomförandet av det nya dataskyddsdirektivet och eftersom direktivet ställer synnerligen heltäckande och detaljerade krav på den nationella lagstiftningen, är det inte ändamålsenligt att i denna proposition närmare beskriva gällande lagstiftning i andra länder. Den gällande lagstiftningen i EU-staterna behandlas i konsekvensanalysen, som kommissionen publicerade i samband med förslaget till direktiv (SEC(2012) 72 final).

Internationella avtal med tredjeländer

Enligt artikel 61 i det nya dataskyddsdirektivet ska internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 6 maj 2016 och som är förenliga med unionsrätten så som den tillämpades före den dagen fortsätta att gälla tills de ändras, ersätts eller återkallas.

4 Bedömning av nuläget

För att det nya dataskyddsdirektivet ska kunna genomföras nationellt måste ny lagstiftning införas. Med beaktande av att avsikten är att upphäva personuppgiftslagen och att allmänna dataskyddsförordningen och den föreslagna nationella lag som kompletterar den å ena sidan och det nya dataskyddsdirektivet och den lagstiftning som genomför det å andra sidan, trots gemensamma grundläggande principer, bildar klart fristående helheter, föreslås det i denna proposition att det stiftas en separat personuppgiftslag som ska iakttas vid behandling av brottmål. Eftersom de myndigheter som tillämpar lagen, i synnerhet polisen, Gränsbevakningsväsendet, Försvarsmakten och Tullen har olika uppgifter, befogenheter och informationssystem, behöver lagstiftningen kompletteras med särskilda bestämmelser för de olika förvaltningsområdena.

Till vissa delar förutsätter bestämmelserna i direktivet ingen ny nationell lagstiftning. Exempel på sådana bestämmelser i direktivet är vissa bestämmelser om tillsynsmyndighetens förfaranden. I fråga om dem behövs det inte tas in nya bestämmelser i lagstiftningen, eftersom det föreskrivs om dessa frågor i de allmänna förvaltningslagar som är tillämpliga i Finland. Enligt vad som förutsätts t.ex. i artikel 52.2 i direktivet ska medlemsstaterna föreskriva att en tillsynsmyndighet som mottagit ett klagomål och inte är behörig i ärendet ska överlämna det till den behöriga myndigheten. Det behöver inte föreskrivas om saken i detta sammanhang, eftersom bestämmelser om överföring av en handling till den behöriga myndigheten finns i 21 § i förvaltningslagen (434/2003).

Direktivet innehåller också bestämmelser t.ex. om vilka uppgifter den dataskyddsstyrelse som inrättats genom allmänna dataskyddsförordningen har på direktivets tillämpningsområde (artikel 51), kommittéförfarande (artikel 58) och kommissionens rapporter (artikel 62). De behöver inte integreras i den nationella lagstiftningen.

Enligt 12 § 2 mom. i grundlagen är handlingar och upptagningar som innehas av myndigheterna offentliga, om inte offentligheten av tvingande skäl särskilt har begränsats genom lag. Var och en har rätt att ta del av offentliga handlingar och upptagningar. Dataskyddsdirektivet gör det möjligt att beakta offentlighetsprincipen i den nationella lagstiftningen. När lagstiftning bereds bör man därför se till att offentlighets- och dataskyddslagstiftningen samordnas. När uppgifter lämnas ut ur en myndighets personregister ska offentlighetsprincipen och sekretessbestämmelserna beaktas på det sätt som föreskrivs i offentlighetslagen och i synnerhet i dess 16 § 3 mom. Bestämmelser om offentlighet för behöriga myndigheters handlingar och i annan verksamhet finns dessutom i speciallagstiftning, såsom i lagen om offentlighet vid rättegång i allmänna domstolar. Avsikten är inte att genom denna proposition ändra det nuvarande rättsläget i detta avseende. På grund av den reviderade dataskyddslagstiftningen och den övriga utvecklingen i samhället är det dock skäl att i framtiden bedöma behovet av att se över den nationella offentlighetslagstiftningen.

5 Målsättning och de viktigaste förslagen

5.1 Målsättning

Syftet med propositionen är att EU:s nya dataskyddsdirektiv genomförs i Finland. I förhållande till det resultat som eftersträvas är direktivet förpliktande för varje medlemsstat det riktar sig till, men överlåter åt de nationella myndigheterna att välja form och medel. Även om dataskyddsdirektivet förutsätter att nationell lagstiftning införs för att genomföra direktivet, ger det dock till vissa delar medlemsstaterna prövningsrätt i synnerhet när det gäller detaljer i lagstiftningen.

I dataskyddsdirektivet konstateras det att det nationella genomförandet inte får leda till försämringar i personuppgiftsskyddet. Direktivet hindrar inte heller medlemsstaterna från att föreskriva om en högre skyddsnivå för skyddet av den registrerades rättigheter än vad som fastställts i direktivet. I denna proposition har hänsyn tagits till bestämmelserna i den gällande personuppgiftslagen och strävan har till vissa delar varit att trygga den registrerades rättigheter på en högre nivå än den miniminivå som förutsätts i direktivet. I den föreslagna genomförandelagen har det t.ex. tagits in bestämmelser om behandling av personbeteckningar, även om dataskyddsdirektivet inte innehåller sådana bestämmelser.

I enlighet med vad som skrivits in i regeringsprogrammet för statsminister Sipiläs regering i fråga om genomförandet av EU-författningar har strävan vid utarbetandet av propositionen varit att avhålla sig från att skapa ytterligare nationell reglering. I propositionen har det dock tagits in allmänna bestämmelser om behandling av personuppgifter vid upprätthållandet av den

nationella säkerheten, eftersom skyddet för personuppgifter till denna del annars skulle bli ofullständigt, även med beaktande av kravet i 10 § 1 mom. i grundlagen enligt vilket närmare bestämmelser om skydd för personuppgifter utfärdas genom lag.

Alla myndigheter som tillämpar den lagstiftning som genomför dataskyddsdirektivet tillämpar också allmänna dataskyddsförordningen i sin verksamhet. Vid beredningen av den föreslagna lagstiftningen har man i syfte att främja en enhetlig lagstiftning därför försökt följa de innehållsmässiga och terminologiska lösningar som använts i förordningen och i regeringens proposition med förslag till lagstiftning som kompletterar förordningen, till den del det inte funnits vägande skäl att stanna för en annorlunda lösning.

5.2 De viktigaste förslagen

Den föreslagna lagens tillämpningsområde

Den föreslagna lagen har karaktären av allmän lag som ska iakttas inom dataskyddet vid behandling av brottmål. Den är subsidiär i förhållande till annan lagstiftning. Om det i någon annan lag finns bestämmelser som avviker från den föreslagna lagen, ska de tillämpas i stället för den föreslagna lagen. Med beaktande av att de behöriga myndigheter som tillämpar lagen har olika uppgifter och befogenheter, kan det anses föreligga ett behov av sektorsspecifik reglering i Finland, och sådan lagstiftning har också beretts samtidigt med denna proposition. Det är klart att den lagstiftning som tillämpas som helhet ska harmoniera med det nya dataskyddsdirektivet och internationella fördrag som är förpliktande för Finland.

Med tanke på när lagen ska tillämpas behöver såväl dess materiella som organisatoriska tillämpningsområde beaktas. Lagen ska tillämpas av myndigheter vars behörighet omfattar förebyggande, utredning och avslöjande av brott eller åklagarverksamhet som har samband med brott, dömande till straffrättsliga påföljder eller verkställande av straffrättsliga påföljder. Sådana myndigheter är bl.a. polisen, Gränsbevakningsväsendet, Tullen, åklagarna, domstolarna och Brottspåföljdsmyndigheten. Dessa myndigheter ska dock tillämpa den föreslagna lagen endast när de behandlar personuppgifter i ovannämnda syfte, dvs. t.ex. i samband med utredning av brott eller vid handläggning av brottmål i domstol. När t.ex. polisen behandlar personuppgifter i samband med ett ansökningsärende, ska allmänna dataskyddsförordningen och den nationella lagstiftning som kompletterar den tillämpas i stället för den föreslagna lagen.

Lagen ska dessutom tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter vid upprätthållandet av den nationella säkerheten. Behöriga myndigheter är till denna del Försvarsmakten, Gränsbevakningsväsendet och polisen, i synnerhet skyddspolisen. Till denna del grundar sig den föreslagna lagens tillämpningsområde inte på genomförandet av direktivet, utan det är fråga om en nationell lösning. Upprätthållandet av den nationella säkerheten faller på grundval av uttryckliga bestämmelser utanför tillämpningsområdet för såväl allmänna dataskyddsförordningen som dataskyddsdirektivet. För att undvika luckor i lagstiftningen om behandling av personuppgifter när det gäller verksamhet som siktar på upprätthållandet av den nationella säkerheten och för att kravet i grundlagens 10 § 1 mom. om att det ska föreskrivas om saken i lag ska bli uppfyllt, ska det på nationell nivå föreskrivas om vilken lagstiftning som ska tillämpas på sådana situationer. I den lag som genomför dataskyddsdirektivet har det jämfört med allmänna dataskyddsförordningen på grund av regleringsobjektet i någon mån lagts större vikt vid myndighetens behov att i vissa situationer begränsa den registrerades rättigheter, såsom den registrerades rätt till insyn. Med beaktande av att det finns motsvarande myndighetsbehov på området för nationell säkerhet, är det ändamålsenligt att den behandling av personuppgifter som sker vid upprätthållandet av den nationella säkerheten tas in i den lag för genomförandet av direktivet som föreslås i denna proposition till den del det inte föreskrivs något annat i speciallagstiftning.

Principer för behandling av personuppgifter

I det föreslagna 2 kap. tas det in bestämmelser om de allmänna förutsättningarna för behandling av personuppgifter på tillämpningsområdet. Den behandling av personuppgifter som sker på den föreslagna lagens tillämpningsområde ska behövas för att den behöriga myndigheten ska kunna sköta de i lag angivna uppgifter som avses i den föreslagna lagen. Den personuppgiftsansvarige får dock behandla personuppgifter också för arkivändamål eller för vetenskapliga, statistiska eller historiska ändamål. De personuppgifter som behandlas ska vara korrekta samt adekvata, uppdaterade och behövliga med tanke på ändamålet med behandlingen. Det ska vid behov och så långt det är möjligt göras åtskillnad mellan personuppgifter som gäller personer i olika ställning, såsom målsägande, vittnen eller misstänkta.

När personuppgifter överförs till en mottagare etablerad inom Europeiska unionen, får den överförande myndigheten inte uppställa strängare krav på behandlingen av personuppgifter än vad som tillämpas nationellt på likartade uppgiftsöverföringar. Den myndighet som överför uppgifterna ska informera mottagaren om skyldigheten att följa eventuella lagstadgade begränsningar vid uppgiftsanvändningen.

I den föreslagna lagen tas det in bestämmelser om särskilda kategorier av personuppgifter. Uppgifter som hör till särskilda kategorier av personuppgifter, som ofta också kallas känsliga uppgifter, är personuppgifter som avslöjar 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. Sådana uppgifter får behandlas endast om det är nödvändigt och under förutsättning att skyddsåtgärder som krävs för att trygga den registrerades rättigheter har vidtagits.

I lagen tas det också in bestämmelser genom vilka behandling av personbeteckningar och anteckning av en personbeteckning i handlingar begränsas. Förslaget grundar sig inte till denna del på det nya dataskyddsdirektivet, utan det är fråga om en nationell lösning. De föreslagna bestämmelserna motsvarar i väsentlig grad bestämmelserna i personuppgiftslagen.

Lagen ska innehålla bestämmelser om automatiserat individuellt beslutfattande. Det nya dataskyddsdirektivet förutsätter att beslut som enbart grundas på automatiserad behandling, inbegripet profilering, och som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under. Den registrerade ska ha rätt att kräva mänskligt ingripande från den personuppgiftsansvariges sida. I Finland fattar t.ex. polisen inga sådana automatiserade individuella beslut av den art som beskrivs ovan. I propositionen föreslås det därför ett förbud mot sådana beslut. Förbudet utgör dock inget hinder för att föreskriva om sådant beslutsfattande någon annanstans i lag. Den lagstiftningen ska då överensstämma med kraven i direktivet.

Den personuppgiftsansvariges och personuppgiftsbiträdets ansvar

Enligt den föreslagna allmänna lagen ska den personuppgiftsansvarige svara för att personuppgifter behandlas i enlighet med lag. Den personuppgiftsansvarige ska vidta behövliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen är laglig. I lagen tas det också in bestämmelser om dataskydd som standard och inbyggt dataskydd samt bestämmelser om ansvarsfördelningen i de situationer då två eller flera personuppgiftsansvariga gemensamt fastställer behandlingens ändamål och medel. De föreslagna bestämmelserna grundar sig på direktivets bestämmelser om att föreskriva om saken i lag.

Personuppgiftsbiträdet, dvs. den som behandlar personuppgifter för den personuppgiftsansvariges räkning, ska enligt den föreslagna lagen ge den personuppgiftsansvarige lämpliga utredningar och förbindelser och även i övrigt tillräckliga garantier för de organisatoriska och tekniska åtgärder genom vilka det säkerställs att personuppgifterna behandlas i enlighet med kraven i lagen. Ett skriftligt avtal ska upprättas över den behandling som personuppgiftsbiträdet utför. I avtalet ska bl.a. behandlingens art, ändamål och varaktighet anges. Det kan bestämmas om dessa omständigheter också genom någon annan rättshandling som är bindande för personuppgiftsbiträdet. Förslagen grundar sig också till denna del på direktivet.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska enligt den föreslagna lagen se till att logguppgifter bevaras över insamling, ändring, läsning, utlämning, överföring, sammanförande och utplåning av personuppgifter som utförts i deras automatiserade behandlingssystem. I lagen tas det också in bestämmelser om en skyldighet att göra en konsekvensbedömning avseende dataskyddet innan behandlingen av personuppgifter inleds. I vissa fall ska konsekvensbedömningen vara skriftlig. Om konsekvensbedömningen visar att behandlingen trots de skyddsåtgärder som den personuppgiftsansvarige planerat kan medföra en betydande risk för den registrerades rättigheter, ska den personuppgiftsansvarige eller personuppgiftsbiträdet höra dataombudsmannen. Om ombudsmannen anser att behandlingen skulle vara lagstridig, ska ombudsmannen enligt huvudregeln inom sex veckor ge den personuppgiftsansvarige eller personuppgiftsbiträdet instruktioner i syfte att göra behandlingen laglig. Även till denna del är det fråga om genomförandet av direktivet.

De registrerades rättigheter

Det föreslås att det i den allmänna lagen föreskrivs om den personuppgiftsansvariges skyldighet att tillhandahålla en dataskyddsbeskrivning som ska göras allmänt tillgänglig. Av beskrivningen ska bl.a. framgå ändamålen med och den rättsliga grunden för behandlingen av personuppgifter, den period under vilken personuppgifterna kan bevaras, sedvanliga mottagare av personuppgifterna samt kontaktuppgifter för den personuppgiftsansvarige och dataskyddsombudet. Bestämmelserna grundar sig delvis på direktivet och delvis på bestämmelserna i personuppgiftslagen och förutsätter att en mer omfattande offentlig beskrivning tillhandahålls än vad som föreskrivs i direktivet. I det nya dataskyddsdirektivet förutsätts det att den information som avses där görs tillgänglig för den registrerade, medan det i den föreslagna allmänna lagen ställs klarare krav på offentliggörandet av beskrivningen.

I den allmänna lagen tas det in bestämmelser om den registrerades rätt till insyn, dvs. om rätt att få veta huruvida personuppgifter som gäller honom eller henne behandlas samt rätt att få sådana uppgifter liksom även information om ändamålen med behandlingen. Den registrerade ska också ha rätt att få sådana personuppgifter om honom eller henne kompletterade eller rättade som är bristfälliga eller felaktiga med tanke på ändamålet med behandlingen. Dessa rättigheter för den registrerade kan dock begränsas, om en begränsning med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd i syfte att undvika menlig inverkan på förebyggande, avslöjande, utredning av brott eller på åtgärder som avser åtal för brott eller på verkställighet av straffrättsliga påföljder, eller om en begränsning av dem är en proportionell och nödvändig åtgärd bl.a. i syfte att skydda den nationella säkerheten. Den registrerade har rätt att be dataombudsmannen att agera för sig i ärendet, om den personuppgiftsansvarige begränsar den registrerades rättigheter på ovannämnda grund. Dataombudsmannen ska inom en rimlig tid informera den registrerade om vilka åtgärder ombudsmannen har vidtagit. De föreslagna bestämmelserna grundar sig till denna del på direktivet.

Artikel 12.4 i direktivet förutsätter att den registrerade ska kunna utöva sina rättigheter kostnadsfritt. Om den registrerades begäranden, t.ex. på grund av att de upprepas, är uppenbart ogrundade eller orimliga, kan den personuppgiftsansvarige dock ta ut en rimlig avgift eller

vägra att tillmötesgå begäran. I den föreslagna allmänna lagen ska det ingå bestämmelser om att den registrerade får utöva sina rättigheter avgiftsfritt. Lagen ska innehålla bestämmelser om möjlighet för den personuppgiftsansvarige att ta ut en avgift enligt lagen om grunderna för avgifter till staten, om den registrerades begäran är uppenbart ogrundad eller orimlig. I propositionen föreslås det inte att den personuppgiftsansvarige i en sådan situation helt får vägra tillmötesgå den registrerades begäran, eftersom rätten till insyn samt rätten att få uppgifter kompletterade eller rättade kan ha en väldigt stor betydelse med tanke på tillgodoseendet av den registrerades rättigheter och eftersom möjligheten att ta ut en avgift i tillräcklig grad kan anses hindra t.ex. upprepade ogrundade begäranden från den registrerade.

Informationssäkerhet

I enlighet med direktivets bestämmelser om att föreskriva om saken i lag tas det i den föreslagna allmänna lagen in bestämmelser om den personuppgiftsansvariges och personuppgiftsbiträdets skyldighet att genom tekniska och organisatoriska åtgärder skydda personuppgifterna på ett sätt som motsvarar den risk för den registrerades rättigheter som behandlingen medför. Personuppgiftsbiträdet ska efter att ha fått vetskap om en personuppgiftsincident utan obefogat dröjsmål informera den personuppgiftsansvarige om incidenten. Den personuppgiftsansvarige ska å sin sida anmäla incidenten till dataombudsmannen, utom när det är osannolikt att personuppgiftsincidenten medför en risk för den registrerades rättigheter. I den allmänna lagen tas det också in bestämmelser om den personuppgiftsansvariges skyldighet att informera den registrerade om en personuppgiftsincident, med vissa undantag som uppräknas i lagen.

Den personuppgiftsansvarige ska enligt den föreslagna allmänna lagen lämna en anmälan om en personuppgiftsincident också till personuppgiftsansvariga i Finland eller i andra EU-medlemsstater, om incidenten gäller personuppgifter som har överförts av eller till de personuppgiftsansvariga i fråga. Direktivet förutsätter endast att det föreskrivs om lämnande av information till personuppgiftsansvariga i andra EU-stater, men i lika hög grad behöver andra personuppgiftsansvariga i Finland informeras om en personuppgiftsincident av nämnda slag.

Överföringar av personuppgifter till tredjeländer

I den allmänna lagen tas det in bestämmelser i enlighet med direktivet om de allmänna förutsättningar under vilka den behöriga myndigheten får överföra personuppgifter till tredjeländer. Överföringen ska för det första vara nödvändig för de ändamål som uppräknas i den föreslagna lagens tillämpningsbestämmelse, t.ex. för utredning av ett brott eller för verkställighet av straff. Kommissionen ska dessutom ha konstaterat att skyddsnivån i landet i fråga är adekvat. Överföring till ett tredjeland är på vissa noggrant angivna villkor möjlig också i en situation då kommissionen inte har fattat beslut om adekvat skyddsnivå för landet i fråga.

Tillsynen över efterlevnaden av lagen

Dataombudsmannen är den specialmyndighet som ska utöva tillsyn över efterlevnaden av lagen. Bestämmelser om dataombudsmannen och dataombudsmannens byrå tas in den dataskyddslag som kompletterar allmänna dataskyddsförordningen. Dataombudsmannen ska också utöva tillsyn över efterlevnaden av den lagen. Det är ändamålsenligt att samma myndighet utövar tillsyn över såväl allmänna dataskyddsförordningen, den dataskyddslag som kompletterar dataskyddsförordningen som den lag som genomför det nya dataskyddsdirektivet, med beaktande av att lagstiftningen bildar en synnerligen enhetlig helhet. I den föreslagna lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten tas det in bestämmelser om dataombudsmannens uppgifter och befogenheter vid tillsynen över efterlevnaden av lagen.

Dataombudsmannen ska utöva tillsyn över efterlevnaden av den föreslagna lagen både på eget initiativ och på basis av begäranden om åtgärder som lämnas in till ombudsmannen. Dataombudsmannen kan göra utredningar av hur lagen följs och behandla begäranden om åtgärder som lämnats in till ombudsmannen. Ombudsmannen kan i fall av ett lagstridigt förfarande t.ex. meddela den personuppgiftsansvarige en anmärkning eller uppställa ett tillfälligt eller bestående förbud eller någon annan tillfällig eller bestående begränsning av behandlingen av personuppgifter. Ombudsmannen kan förena ett rättsligt förpliktande beslut med vite.

Dataombudsmannen ska utöver tillsynsuppgifter ha handledande uppgifter och uppgifter som främjar skyddet av personuppgifter. Dataombudsmannen ska öka allmänhetens medvetenhet om risker, lagstiftning, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter. Ombudsmannen ska också på begäran ge de registrerade information om hur de ska utöva sina rättigheter. Ombudsmannen ska också öka de personuppgiftsansvarigas och personuppgiftsbiträdenas medvetenhet om vilka skyldigheter de har samt ge dem råd vid förfarandet med förhandssamråd.

Även justitiekanslern i statsrådet och riksdagens justitieombudsman ska övervaka efterlevnaden av den föreslagna lagstiftningen som en del av den allmänna laglighetskontrollen av myndigheternas och tjänstemännens verksamhet. De ska också övervaka sådan behandling av personuppgifter som domstolarna utför i samband med sina rättskipningsuppgifter, även om det inte föreslås att tillsynen över domstolarnas verksamhet ska ingå i dataombudsmannens behörighet.

Rättssäkerhet och påföljder

Det föreslås att det i den allmänna lagen tas in bestämmelser om en skyldighet för den behöriga myndigheten att införa förfaranden som gör det möjligt att konfidentiellt till myndigheten rapportera överträdelser av bestämmelserna om skydd för personuppgifter. Genom en sådan låg tröskel för att ta kontakt (angivningssystem kallat whistleblowing) uppmuntras personer som upptäcker missförhållanden att rapportera saken direkt till den behöriga myndigheten för att denna på eget initiativ ska kunna vidta lämpliga korrigerande eller andra åtgärder.

Ett synnerligen viktigt förfarande i praktiken med tanke på den registrerades rättssäkerhet är möjligheten att lämna in en begäran om åtgärder avseende ett misstänkt olagligt förfarande till dataombudsmannen. Med den registrerades samtycke får en begäran om åtgärder lämnas in till dataombudsmannen för behandling också av ett allmännyttigt samfund som främjar skyddet av personuppgifter. Dataombudsmannen ska pröva begäran om åtgärder till behövliga delar och inom rimlig tid informera den som inlett ärendet om hur behandlingen fortskrider och om resultatet. Ombudsmannen kan på ovannämnt sätt t.ex. förbjuda behandling av personuppgifter. Ombudsmannens beslut får överklagas genom besvär hos förvaltningsdomstolen.

Enligt artikel 56 i direktivet ska medlemsstaterna föreskriva om den registrerades rätt att få ersättning för materiell eller immateriell skada som han eller hon lidit till följd av ett olagligt förfarande. Det föreslås bestämmelser om att den personuppgiftsansvarige ska vara skyldig att ersätta den registrerade eller någon annan person för ekonomisk skada eller annan skada som denne har tillfogats av att personuppgifter har behandlats i strid med den föreslagna allmänna lagen. Den registrerade kan också få möjlighet att kräva sådan ersättning för lidande som avses i skadeståndslagen (412/1974). Enligt 5 kap. 6 § i skadeståndslagen har den vars privatliv har kränkts genom en straffbar handling rätt till ersättning för lidande som orsakats av kränkningen.

Enligt artikel 57 i direktivet ska medlemsstaterna föreskriva om effektiva, proportionella och avskräckande sanktioner för överträdelser av dataskyddsbestämmelserna. Allmänna data-

skyddsförordningen föreskriver för sin del om en administrativ påföljdsavgift (”administrativ sanktionsavgift”) som påföljd för brott mot de dataskyddsbestämmelser som avses i den. Myndigheterna kan dock helt eller delvis utesluta användningen av en sådan. I den föreslagna allmänna lagen tas det in hänvisningsbestämmelser till de bestämmelser i strafflagen som gäller kränkning av kommunikationshemlighet, dataintrång, brott mot tystnadsplikt och tjänstebrott samt grova gärningsformer av dem.

I propositionen föreslås det inte att en administrativ påföljdsavgift ska införas på den föreslagna allmänna lagens tillämpningsområde. Med beaktande av dataombudsmannens möjlighet att utfärda rättsligt bindande förelägganden som avser den personuppgiftsansvarige eller personuppgiftsbiträdet samt möjligheten att förena dem med vite, den registrerades rätt att få ersättning för skada som han eller hon lidit samt strafflagens bestämmelser om tjänstebrott och andra straffbestämmelser, behöver en påföljdsavgift inte införas på den föreslagna lagens tillämpningsområde. I propositionen föreslås det mer omfattande befogenheter för dataombudsmannen än minimikravet i direktivet, vilket för sin del möjliggör ett större urval metoder när det gäller att ingripa i lagstridig behandling av personuppgifter. Att föreskriva om en administrativ påföljdsavgift av straffkaraktär som påföljd för ett lagstridigt förfarande i myndighetsverksamhet kan inte heller anses vara en normal lösning i vårt rättssystem.

Europeiska kommissionen kan i enlighet med artikel 35 och 36 i direktivet besluta att ett tredjeland har en adekvat skyddsnivå med tanke på överföring av personuppgifter. I artikel 36 föreskrivs det bl.a. om de omständigheter som kommissionen ska beakta när den fattar beslutet. Den nationella tillsynsmyndigheten kan inte pröva lagligheten i kommissionens beslut, eftersom ärendet hör till EU-domstolens exklusiva befogenhet.

Europeiska unionens domstol ansåg i sitt förhandsavgörande i målet Schrems (C-362/14) att det är den nationella lagstiftarens sak att föreskriva om de rättsmedel med vilka den nationella tillsynsmyndigheten i fråga kan föra fram de grunder som myndigheten finner motiverade i de nationella domstolarna, för att dessa vid behov kan begära ett förhandsavgörande av Europeiska unionens domstol för prövning av giltigheten av kommissionens beslut. Det finns alltså ett behov av bestämmelser i den nationella lagstiftningen för att de kommissionsbeslut som avses här ska kunna bedömas hos den nationella tillsynsmyndigheten och i domstol. I den föreslagna allmänna lagen tas det därför in bestämmelser om att dataombudsmannen genom en ansökan kan föra ett sådant ärende till Helsingfors förvaltningsdomstol för avgörande. Förvaltningsdomstolen kan för sin del vid behov begära EU-domstolens förhandsavgörande beträffande lagenligheten i kommissionens beslut. Eftersom dessa ärenden antagligen kommer att vara få till antalet är det skäl att koncentrera behandlingen av dem till Helsingfors förvaltningsdomstol.

Ikraftträdande och övergångsbestämmelser

Enligt artikel 63 i dataskyddsdirektivet ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa direktivet. Medlemsstaterna ska också tillämpa dessa bestämmelser från och med nämnda datum. Av den anledningen föreslås det att de lagar som ingår i propositionen ska träda i kraft den 6 maj 2018 eller så snart som möjligt efter det.

I artikel 63 i det nya dataskyddsdirektivet föreskrivs det att en medlemsstat får skjuta upp ikraftträdandet av ovannämnda loggningsskyldighet till senast den 6 maj 2023, om skyldigheten skulle innebära oproportionella ansträngningar. Under exceptionella omständigheter och om fullgörandet av skyldigheten skulle innebära allvarliga problem för driften av detta automatiska behandlingssystem, kan ikraftträdandet av skyldigheten skjutas upp till senast den 6 maj 2026. Möjligheten ska i bägge fallen endast gälla sådana automatiserade behandlingssy-

stem som har inrättats före den 6 maj 2016. Med beaktande av att endast få av de informationssystem som skapats i Finland före den 6 maj 2016 uppfyller de krav på loggning som ingår i det nya dataskyddsdirektivet, och med beaktande av de tidsmässiga och ekonomiska resurser som skapandet av ett loggningssystem kräver, föreslås det att det föreskrivs att system som har skapats före den 6 maj 2016 ska bringas i överensstämmelse med bestämmelserna om logguppgifter senast den 6 maj 2023.

Övriga lagförslag

I propositionen ingår föreslag till ändring av vissa lagar på justitieministeriets ansvarsområde till följd av det nationella genomförandet av direktivet. I lagarna stryks hänvisningarna till personuppgiftslagen, som upphävs, och ersätts vid behov med en hänvisning till den föreslagna allmänna lagen, allmänna dataskyddsförordningen samt dataskyddslagen. I lagarna stryks sådana bestämmelser som är överlappande med den föreslagna allmänna lagen, såsom den registrerades rätt till insyn. I fråga om vissa lagar sägs det klarare vilken myndighet som ska anses vara personuppgiftsansvarig för ett visst register.

I ändringslagarna föreslås det vissa terminologiska preciseringar. Av konsekvensskäl föreslås det att den svenska språkdräkten i de aktuella bestämmelserna i ändringslagarna ändras så att termen ”registeransvarig” systematiskt ändras till termen ”personuppgiftsansvarig”.

6 Propositionens konsekvenser

6.1 Ekonomiska konsekvenser

Allmänt

Propositionens ekonomiska konsekvenser riktar sig i huvudsak till de behöriga myndigheter som är personuppgiftsansvariga. Den föreslagna lagstiftningen har nästan inga konsekvenser för företagens verksamhet. De ekonomiska konsekvenserna beror i regel direkt på dataskyddsdirektivet.

Konsekvenser för förvaltningen

Dataskyddsdirektivet förutsätter att den personuppgiftsansvarige utser ett dataskyddsombud. Detta medför direkta kostnader för en del av de personuppgiftsansvariga. De direkta ekonomiska konsekvenserna av skyldigheten att utse ett dataskyddsombud minskas av att två eller flera personuppgiftsansvarige kan utse ett gemensamt dataskyddsombud och att dataskyddsombudet kan sköta både uppgifter som följer av den föreslagna lagen och uppgifter som följer av allmänna dataskyddsförordningen. En del myndigheter, såsom polisen, har redan från tidigare ett dataskyddsombud, så betydande extra kostnader borde inte uppstå för polisen i detta avseende. Domstolarna samt justitiekanslern i statsrådet och riksdagens justitieombudsman är befriade från skyldigheten att utnämna ett dataskyddsombud i fråga om sina rättskipnings- och lagövervakningsuppgifter..

I den föreslagna lagstiftningen åläggs den personuppgiftsansvarige olika skyldigheter när det gäller att informera, dokumentera samt föra register och tillhandahålla beskrivningar. Dessa förorsakar en viss administrativ börda. Å andra sidan ingår motsvarande skyldigheter delvis redan i den gällande lagstiftningen. Verkställigheten av den föreslagna lagstiftningen leder också till att det behövs utbildning och information av myndigheterna.

Konsekvenser för informationssystemen

De krav som ingår i dataskyddsdirektivet har direkta och indirekta konsekvenser för de nationella informationssystemen. Kostnadsverkningarna av kraven i direktivet kan som helhet vara betydande till den del det är fråga om sådana obligatoriska skyldigheter som inte tidigare har genomförts i informationssystemen. Kostnaderna varierar dock hos olika personuppgiftsansvariga bl.a. beroende på hur respektive nuvarande informationssystem fungerar samt sättet och tidtabellen för att fullgöra de skyldigheter som anges i lag. En del av skyldigheterna kan verkställas också genom att arbetsmetoder och praxis ändras.

Direkta och indirekta kostnadsverkningar kan följa särskilt av de krav som gäller åtskillnad mellan olika kategorier av personer i systemet, precisare förutsättningar för behandling av känsliga personuppgifter, strävan att skilja personuppgifter som grundar sig på personliga bedömningar från personuppgifter som grundar sig på fakta, anteckning om begränsning av användningen av personuppgifter (på begäran av den registrerade eller någon annan myndighet eller en myndighet i en annan medlemsstat), logguppgifter och precisare krav på informationssäkerhet.

Det krav i fråga om informationssystemen som har de största kostnadsverkningarna gäller loggsystemen. I propositionen konstateras det i fråga om loggsystemen att den övergångsperiod som tillåts i direktivet införs, dvs. att informationssystemen till denna del ska motsvara kraven i direktivet senast den 6 maj 2023. De exakta kostnadsverkningarna av att informationssystemen förnyas beror även i övrigt på hur man i praktiken beslutar genomföra de jämförelsevis allmänt utformade rättsliga krav som ställs på systemen.

Polisens informationssystem

Inom polisen används flera informationssystem som omfattas av dataskyddsdirektivets tillämpningsområde. Skyldigheten att göra åtskillnad mellan olika kategorier av personer i brottmål grundar sig redan på den tidigare rekommendationen av Europarådet, likaså skyldigheten att skilja uppgifter som grundar sig på fakta från personuppgifter som grundar sig på personliga bedömningar. Dessa skyldigheter innehåller också i viss mån rörelseutrymme. I polisens informationssystem uppfylls kraven till största delen redan nu, men i fråga om vissa system kan utvecklingsåtgärder vidtas. I polisens nya informationssystem föreslås det att kravet uppfylls vid behov i samband med reformprojekt inom ramen för deras tidtabell för genomförandet.

De särskilda förutsättningar som hänför sig till behandling av personuppgifter (skyldighet att informera, begränsningar i fråga om utlämnande av uppgifter) har direkta ekonomiska konsekvenser. Även till den del det är fråga om rättelse och utplåning av personuppgifter och begränsning av behandlingen, kommer genomförandet av kraven i direktivet att ha direkta kostnadsverkningar för polisens informationssystem. Alla de olika funktioner som behövs har inte genomförts i polisens informationssystem. Kraven ingår redan i det gällande dataskyddsrambeslutet, så en ändring av innehållet i lagstiftningen är inte särskilt betydande i detta avseende. En del av kraven kan dock vara svåra att uppfylla i tekniskt avseende eller rent omöjliga att uppfylla till fullo, och kostnadsverkningarna kan variera från skäliga till betydande, beroende på hur direktivet tolkas och sättet att genomföra det tekniskt. I fråga om polisens informationssystem beror kostnadsverkningarna på hur strikt kravet på loggar över läsning i systemen tolkas. Kostnadsverkningarna kan dock vara betydande i fråga om ett enskilt informationssystem. I fråga om nya systemprojekt ska skyldigheterna avseende logguppgifter beaktas, även med beaktande av den övergångsperiod som står till buds.

I fråga om inbyggt dataskydd och dataskydd som standard har man strävat efter att genomföra polisens samtliga befintliga informationssystem så att de väntas uppfylla kraven i direktivet. Vissa krav som avviker från den gällande lagen och som innebär en stramare reglering väntas

dock medföra behov att ändra praxis på ett sätt som kan leda till kostnadsverkningar. De hänför sig särskilt till hot mot informationssäkerhet och beredskap inför sådana samt bedömning av risken vid behandling av personuppgifter. Krav som har samband med säkerheten vid behandlingen har i regel beaktats i polisens informationssystem. Det är dock möjligt att de krav som hänför sig till hotbilder och bedömning av riskerna vid behandlingen förorsakar rimliga behov av ändringar i informationssystemen. I fråga om polisens informationssystem har man gjort bedömningen att skyldigheten att anmäla en personuppgiftsincident till en annan myndighet eller en annan myndighet i en EU-medlemsstat kan medföra behov av ändringar.

Tullen

I Tullens informationssystem förekommer det behandling av personuppgifter som hänför sig till såväl direktivets som förordningens tillämpningsområde. Den behandling av personuppgifter inom Tullen som omfattas av direktivets tillämpningsområde sker till stor del i de tekniska tillämpningar som polisen upprätthåller (informationssystemet för polisärenden och informationssystemet för misstänkta). Till denna del svarar polisen för att informationssystemen överensstämmer med direktivet. Enligt en preliminär bedömning krävs det inte systemändringar i Tullens register för att kraven i den föreslagna lagen ska uppfyllas, och betydande kostnader uppkommer därmed inte.

Gränsbevakningsväsendet

Den behandling av personuppgifter inom Gränsbevakningsväsendet som omfattas av direktivets tillämpningsområde sker i regel i de tekniska tillämpningar som polisen upprätthåller (informationssystemet för polisärenden och informationssystemet för misstänkta). Till denna del svarar polisen för att informationssystemen överensstämmer med direktivet. I fråga om personregister vid enskilda brottsbekämpningsenheter finns det skäl att bedöma till vilka delar dessa lagringsplattformar uppfyller kraven i den föreslagna genomförandelagen, och göra behövliga ändringar antingen i lagringsplattformarna eller mer allmänt i sättet att behandla personuppgifter. De viktigaste frågor som behöver utredas och som också kan ha kostnadsverkningar gäller rättelse eller utplåning av personuppgifter eller begränsning av behandlingen samt kraven på logguppgifter. Enligt en preliminär bedömning kommer uppfyllandet av de övriga kraven i den föreslagna lagen inte att medföra betydande kostnader för Gränsbevakningsväsendet, eftersom kraven i regel är uppfyllda redan nu.

Försvarsmakten

Försvarsmakten håller på närvarande på att reformera alla sina stora informationssystem. Reformarbetet inleddes redan före EU:s dataskyddsreform, och den föreslagna lagen väntas ha endast ringa effekter på de informationssystem som nu håller på att utvecklas inom Försvarsmakten. Med beaktande av övergångsperioderna fordrar de ändringsbehov som följer av den föreslagna lagen dock ingen tilläggsfinansiering. För Försvarsmakten är kostnadsverkningarna av ett dataskyddsombud 1 årsverke. Detta är en följd dels av den föreslagna genomförandelagen, dels av allmänna dataskyddsförordningen.

Justitieministeriets förvaltningsområde

I Rättsregistercentralens informationssystem (straffregistret, systemet Rajsa för verkställighet av böter och systemet CRIS för utbyte av straffregisteruppgifter inom EU) måste det göras ändringar på grund av den föreslagna lagen. Kostnader uppstår t.ex. av den skyldighet att föra loggar och de högre krav på informationssäkerhet som ingår i lagförslaget. Engångskostnaderna för de ändringar som krävs i ovannämnda system uppskattas till 500 000 — 600 000 euro och merkostnaderna för kontinuerlig service till 20 000 — 40 000 euro per år. De mest bety-

dande kostnaderna uppstår när skyldigheten att föra logga genomförs i systemet för verkställighet av böter. Dessa bedömningar samt tidtabellen för genomförandet av reformerna, även med beaktande av den övergångsperiod som står till buds, ska preciseras efter det att den nya lagstiftningen har trätt i kraft.

Den föreslagna lagen har också andra konsekvenser för informationssystemen på justitieministeriets förvaltningsområde, såsom för Brottspåföljdsmyndighetens informationssystem. Systemet Sakari, som för närvarande används av åklagarna och domstolarna vid handläggning av brottmål, uppfyller t.ex. inte kraven i den föreslagna genomförandelagen i fråga om skyldigheten att föra loggar. Genom det pågående projektet för att utveckla ärende- och dokumenthanteringen inom åklagarväsendet och vid de allmänna domstolarna (s.k. AIPA-projektet) skapas ett nytt enhetligt system där åklagarna och de allmänna domstolarna elektroniskt behandlar alla sina funktioner kring rättskipningsärenden. AIPA ersätter de separata system som för närvarande används i dessa ärenden, inklusive systemet Sakari för handläggning av brottmål. Avsikten är att i samband med utvecklandet av systemet beakta de krav som ställs på informationssystemen i den föreslagna lagstiftningen. AIPA-projekt ska i sin helhet vara slutfört före utgången av november 2021.

Den föreslagna lagen har konsekvenser för den nationella tillsynsmyndigheten, dvs. dataombudsmannen. Konsekvenserna är dock relativt måttliga jämfört med konsekvenserna av allmänna dataskyddsförordningen. Ekonomiska konsekvenser följer främst på grund av de nya uppgifter som anges i den föreslagna lagen. Sådana är förfarandet med förhandssamråd enligt 21 §, information och rådgivning i synnerhet i samband med lagens ikraftträdande, möjligheten enligt 29 § att utöva rätten till insyn via dataombudsmannen, behandlingen av personsäkerhetsincidenter enligt 34 § samt deltagande i ömsesidigt bistånd mellan dataskyddsmyndigheterna och i internationellt samarbete. Vid dataombudsmannens byrå används för närvarande ca 1,5 årsverken för uppgifter som omfattas av dataskyddsdirektivets tillämpningsområde. Det behov av tilläggsanslag per år som den föreslagna lagen förorsakar dataombudsmannen uppgår till 100 000 euro räknat från 2019, av vilket 80 000 euro förorsakas av löneutgifter (1 årsverke) och 20 000 euro förorsakas av allmänna kostnader (t.ex. publikationsverksamhet). Behovet av tilläggsanslag för 2018 uppskattas till 60 000 euro, vilket beror på tidpunkten då lagen avses träda i kraft.

Ett dataskyddsombud behöver också utses på justitieministeriets förvaltningsområde. Exempelvis Brottspåföljdsmyndigheten bedömer att utnämning av ett dataskyddsombud skapar ett behov av ytterligare 0,7 årsverken. De föreslagna bestämmelserna ökar i någon mån Rättsregistercentralens arbetsmängd bl.a. till följd av att centralen får ansvar för förvaltningen av uppgifterna i delsystemen. Det är dock svårt på förhand att uppskatta vilka kostnader som förorsakas av detta.

6.2 Konsekvenser för myndigheterna

Reformen av EU:s dataskyddslagstiftning innebär en ökad administrativ börda för de personuppgiftsansvariga. En administrativ börda tros uppstå då de registrerade till följd av större medvetenhet om dataskyddsbestämmelser och starkare befogenheter för tillsynsmyndigheterna börjar utöva sina rättigheter aktivare än tidigare. Det är dock svårt att bedöma i vilken utsträckning de registrerade kommer att utöva sina rättigheter. Kostnadsverkningarna hänför sig i huvudsak till skötseln av dataskyddsombudens uppgifter, men eventuellt också till företrädande av den personuppgiftsansvarige i förvaltningsrättsliga och straffrättsliga förfaranden. Med beaktande av att den registrerades rättigheter har effektiviserats också i hela EU så att det i bestämmelserna uttryckligen tagits hänsyn till utövande av rättsmedel också i gränsöverskridande fall och så att dataskyddsmyndigheternas befogenheter utvidgats till att gälla hela EU,

blir de personuppgiftsansvariga eventuellt tvungna att även resursmässigt bereda sig på att dessa rättigheter kommer att utövas.

Å andra sidan ingår en del av skyldigheterna redan i de gällande bestämmelserna, och den totala effekten kan därför anses skälig till denna del. Den personuppgiftsansvarige ska dock t.ex. göra en konsekvensbedömning avseende dataskydd av nya åtgärder för behandling av personuppgifter, vilket inte ingår i den gällande lagstiftningen som en uttrycklig skyldighet. Den personuppgiftsansvarige förorsakas administrativ börda också av att personuppgiftsbiträdena förankras i de nya kraven genom att avtal förnyas. I EU:s dataskyddslagstiftning beaktas förhållandet och de inbördes skyldigheterna mellan den personuppgiftsansvarige och personuppgiftsbiträdena mer ingående än tidigare.

6.3 Samhälleliga konsekvenser

Dataskyddsdirektivet syftar till att underlätta det fria flödet av personuppgifter mellan behöriga myndigheter inom EU när det är fråga om förebyggande, avslöjande och utredning av brott eller åklagarverksamhet i samband med brott eller verkställighet av straffrättsliga påföljder och överföring av sådana uppgifter till tredjeländer och internationella organisationer. Strävan har samtidigt å andra sidan varit att säkerställa ett starkare och mer konsekvent skydd för personuppgifter, vilket stöds genom ett effektivt genomförande.

Europeiska kommissionen har i sin konsekvensbedömning på EU-nivå fäst vikt vid att en enhetligare och mer detaljerad reglering av behandlingen av personuppgifter i brottmål inom hela EU skapar klarhet i rättsläget och förbättrar företagens förtroende för polisens behandling av personuppgifter. Detta har av kommissionen ansetts ha betydelse i synnerhet i situationer då tillsynsmyndigheten är i direkt kontakt med företag som är etablerade på EU:s territorium för att få eller lämna ut personuppgifter när tjänster tillhandahålls över gränserna. Å andra sidan uppmuntrar de nya dataskyddsbestämmelserna dock på lång sikt till att utveckla informationssystemen så att de blir tryggare och informationssäkrare. Dessutom kan en mer ingående reglering av behandlingen av personuppgifter och av tillsynen av behandlingen antas sänka riskerna för dataskyddsförseelser och personuppgiftsincidenter.

De samhälleliga konsekvenserna av de bestämmelser genom vilka dataskyddsdirektivet genomförs kan bedömas också i förhållande till dataskyddsrambeslutet, som upphävs genom direktivet. De problem som kommissionen främst lyft fram i fråga om dataskyddsrambeslutet anknyter till rättsaktens begränsade tillämpning och andra luckor i regleringen. Dessa kommer enligt kommissionens bedömning att konkretiseras när samarbetet inom EU och EU:s gränsöverskridande samarbetet ökar. Regleringen har också ansetts splittrad, om man ser till skillnaderna vid genomförandet av dataskyddsrambeslutet. I dataskyddsdirektivet, som ersätter rambeslutet, har strävan varit att avskaffa den splittrade regleringen så att tillämpningsområdet utvidgas till att gälla all behandling av personuppgifter i brottmål oberoende av om det är fråga om gränsöverskridande överföringar av personuppgifter eller nationell behandling. Målet har varit att säkerställa att individens rättigheter garanteras fullt ut, samt samtidigt förbättra förtroendet för polissamarbetet och underlätta det. Genom det nya direktivet har man också försökt se till att enhetliga och konsekventa principer tillämpas på all behandling av personuppgifter. Samma krav måste beaktas också vid internationella överföringar av personuppgifter.

7 Beredningen av propositionen

År 2016 tillsatte inrikesministeriet, försvarsministeriet och finansministeriet projekt för att genomföra dataskyddsdirektivet på respektive förvaltningsområde. Vid diskussioner mellan ministerierna märkte man emellertid att dataskyddsdirektivet till största delen innehåller sådan allmän reglering som det vid det nationella genomförandet av direktivet är befogat att samla i

en enda allmän lag. Den allmänna lagen ska tillämpas på alla förvaltningsområden som omfattas av direktivets tillämpningsområde. På så sätt undviks överlappande bestämmelser för ett enskilt förvaltningsområde och eventuella ogrundade skillnader i lagstiftningen. De ändringar gällande myndigheternas registersystem och om annan databehandling som behövs i speciallagar om behandling av personuppgifter har beretts separat på respektive förvaltningsområde.

Justitieministeriet tillsatte den 12 januari 2017 en arbetsgrupp med uppgift att bereda ett förslag till den allmänna lagstiftning som behövs för att genomföra dataskyddsdirektivet samt förslag till de ändringar i lagstiftningen på justitieministeriets förvaltningsområde som direktivet förutsätter. Arbetsgruppen skulle också utreda huruvida den aktuella allmänna lagstiftningen kan tillämpas på sådan verksamhet som faller utanför dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde, men där det är motiverat att anpassa regleringen till den övriga reglering som gäller säkerhetsmyndigheter. Företrädda i arbetsgruppen var justitieministeriet, inrikesministeriet, försvarsministeriet, finansministeriet, dataombudsmannen, Rättsregistercentralen och Riksåklagarämbetet.

Arbetsgruppens mandatperiod inföll 16.1—29.9.2017. Arbetsgruppens betänkande överlämnades och publicerades den 6 november 2017 (justitieministeriet, betänkanden och utlåtanden 52/2017). För att direktivet ska kunna genomföras nationellt föreslog arbetsgruppen i sitt betänkande att det stiftas en lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Arbetsgruppen föreslog att lagen ska tillämpas också när Försvarsmakten, polisen och Gränsbevakningsväsendet behandlar personuppgifter i samband med upprätthållandet av den nationella säkerheten. Det är till denna del fråga om en nationell lösning. Arbetsgruppen föreslog också vissa ändringar i lagstiftningen inom justitieministeriets ansvarsområde för att direktivet ska kunna genomföras på förvaltningsområdet.

Arbetsgruppens betänkande genomgick remissbehandling 7.11.2017—4.12.2017. Sammanlagt 33 aktörer yttrade sig om det. Begäran om utlåtande och de inkomna remissvaren finns på webbplatsen utlatande.fi och på statsrådets tjänst för projektinformation.

Remissinstanserna ansåg att förslaget och dess mål kan understödas. Även förslaget om att lagen ska tillämpas på sådan behandling av personuppgifter som sker vid upprätthållandet av den nationella säkerheten understöddes. Det fördes dock fram en mängd anmärkningar om enskilda förslag till bestämmelser och motiveringarna till dem.

Beredningen av propositionen har efter remissbehandlingen fortsatt som tjänsteuppdrag vid justitieministeriet. De grundläggande lösningarna i propositionen har inte ändrats jämfört med arbetsgruppens betänkande. Under den fortsatta beredningen har propositionen dock preciserats och till vissa delar bearbetats jämfört med arbetsgruppens förslag. Dessutom har propositionen setts över för att i väsentliga delar motsvara lösningarna i regeringens proposition med förslag till dataskyddslag (RP 9/2018 rd), t.ex. i fråga om de bestämmelser som gäller tillsynsmyndigheten. De mest betydande innehållsmässiga ändringarna jämfört med arbetsgruppens förslag har gjorts i 8 och 9 kap. i lagförslag 1. Under den fortsatta beredningen har dessutom de ändringar som gällde utsökningsbalken strukits i propositionen. Under den fortsatta beredningen kom man fram till att den behandling av personuppgifter som sker inom ramen för den lagen omfattas av allmänna dataskyddsförordningens tillämpningsområde.

8 Samband med andra propositioner

Propositionen har samband med regeringens proposition med förslag till nationell lagstiftning som kompletterar EU:s allmänna dataskyddsförordning. Justitieministeriet tillsatte i februari 2016 en arbetsgrupp (TATTI, OM006:00/2016) för att bereda de ändringar som den allmänna dataskyddsförordningen förutsätter i den allmänna nationella lagstiftningen om behandling av

personuppgifter. Arbetsgruppen skulle särskilt bereda ett förslag till lagstiftning om nationell tillsynsmyndighet. Arbetsgruppen överlämnade sitt betänkande den 21 juni 2017. Efter det fortsatte beredningen av nämnda lagstiftning som tjänsteuppdrag vid justitieministeriet. Regeringens proposition överlämnades till riksdagen den 1 mars 2018 (RP 9/2018 rd). Propositionen innehåller ett förslag till dataskyddslag, i vilken det tas in bestämmelser om dataombudsmannens organisation. I föreliggande proposition har det därför i fråga om dataombudsmannen endast tagit in bestämmelser om dennes uppgifter och befogenheter på den föreslagna allmänna lagens tillämpningsområde.

Propositionen har också samband med det beredningsarbete som Ålands landskapsstyrelse utför när det gäller vilka ändringsbehov som följer av allmänna dataskyddsförordningen och dataskyddsdirektivet.

Det förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten som ingår i föreliggande proposition är en lag som blir tillämplig som allmän lag på sitt tillämpningsområde. Avsikten är att den ska kompletteras med speciallagstiftning för olika förvaltningsområden på det sätt som anges nedan. Största delen av de propositionerna kommer att överlämnas efter denna proposition.

Propositionen har samband med arbetet i en av inrikesministeriet tillsatt arbetsgrupp (SM064:00/2015) där avsikten är att utarbeta ett förslag till regeringsproposition med förslag till lag om behandling av personuppgifter i polisens verksamhet. Projektets viktigaste syfte är att bereda en ny lag om behandling av personuppgifter i polisens verksamhet. Den blir ett komplement till den allmänna lagstiftningen för genomförandet av dataskyddsdirektivet och till allmänna dataskyddsförordningen till den del de genomförandebestämmelser som behövs inte ingår i de rättsakterna. Avsikten är att polisens nya personuppgiftslag ska uppfylla kraven i den reviderade dataskyddslagstiftningen i EU, med beaktande av behovet av brottsbekämpning samt de krav som de grundläggande och mänskliga rättigheterna ställer.

Propositionen har samband med arbetet i en av inrikesministeriets tillsatt arbetsgrupp (SM057:00/2016) som har till uppgift att utarbeta en regeringsproposition med förslag till 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 bestämmelser som behövs inte ingår i den nationella lagen för genomförande av dataskyddsdirektivet. Dessutom ska arbetsgruppen bedöma vilka andra ändringsbehov som följer av EU:s nya dataskyddslagstiftning samt se över de bestämmelser i sjöräddningslagen som gäller behandling av personuppgifter.

Propositionen har samband med ett av finansministeriet tillsatt projekt (VM059:00/2016) där avsikten är att ändra lagstiftningen om behandling av personuppgifter inom Tullen så att den motsvarar allmänna dataskyddsförordningen och dataskyddsdirektivet till den del de ändringsbehov som följer av den senare inte tillgodoses genom den allmänna lagstiftningen för genomförande av dataskyddsdirektivet.

Propositionen har också samband med arbetet i en av försvarsministeriet tillsatt arbetsgrupp (PLM006:00/2016) där det bereds en totalrevidering av lagstiftningen om behandling av personuppgifter inom försvarsförvaltningen. Arbetsgruppen ska utreda vilka ändringsbehov som följer av EU:s dataskyddsreform för den lagstiftning som gäller behandling av personuppgifter inom försvarsförvaltningen och bereda ett förslag till behövliga ändringar av bestämmelserna. Regeringens proposition i saken överlämnades till riksdagen den 8 mars 2018 (RP 13/2018 rd).

DETALJMOTIVERING

1 LAGFÖRSLAG

1.1 Lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten

1 kap. Allmänna bestämmelser

1 §. *Tillämpningsområde*. I paragrafen föreskrivs det om den föreslagna lagens tillämpningsområde. Bestämmelser om dataskyddsdirektivets tillämpningsområde finns i artikel 1 och 2 i direktivet, på vilka också den föreslagna tillämpningsbestämmelsen i huvudsak grundar sig.

Enligt *1 mom.* ska den föreslagna lagen tillämpas vid sådan behandling av personuppgifter som utförs av de behöriga myndigheter som anges i lagen när det är fråga om förebyggande, avslöjande och utredning av brott eller förande av brott till åtalsprövning (*1 punkten*), åtalsprövning och annan åklagarverksamhet som har samband med brott (*2 punkten*), handläggning av brottmål i domstol (*3 punkten*), verkställighet av straffrättsliga påföljder (*4 punkten*) eller skydd mot eller förhindrande av hot mot den allmänna säkerheten i samband med verksamhet som avses i 1—4 punkten (*5 punkten*).

Enligt skäl 12 i ingressen i dataskyddsdirektivet är polisens och andra brottsbekämpande myndigheters verksamhet främst 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. Denna verksamhet kan också omfatta användning av de befogenheter som föreskrivits för polisen i polislagen eller någon annanstans i lagstiftningen, t.ex. i samband med demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning.

Sådana behöriga myndigheter som avses i den föreslagna lagen är bl.a. polismyndigheterna, tullmyndigheterna, Gränsbevakningsväsendet, domstolarna, åklagarväsendet, Rättsregistercentralen samt Brottspåföljdsmyndigheten. Dessutom är t.ex. riksdagens justitieombudsman och justitiekanslern sådana behöriga myndigheter som avses i den föreslagna lagen, eftersom de enligt 110 § i grundlagen har åtalsrätt. Den föreslagna lagen ska tillämpas på behöriga myndigheter dock endast till den del de utför behandling av personuppgifter för de uppgifter som uppräknas i 1 §.

De behöriga myndigheterna får i den nationella lagstiftningen anförtros också sådana uppgifter som inte utförs för att förebygga, utreda, avslöja eller bedriva åklagarverksamhet i samband med brott, inklusive att skydda mot och förebygga hot mot den allmänna säkerheten. Behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas då av tillämpningsområdet för förordning (EU) 2016/679, dvs. s.k. allmänna dataskyddsförordningen.

Exempelvis polisen har flera uppgifter som omfattas av dataskyddsdirektivets och den föreslagna lagens tillämpningsområde, såsom förundersökning av brott. Polisen sköter dock också andra uppgifter än sådana som hänför sig till brottsbekämpning, såsom vid behandling av passansökningar. På sådan behandling ska den föreslagna lagen inte tillämpas, utan då tillämpas allmänna dataskyddsförordningen och den nationella lagstiftning som kompletterar den. Den föreslagna lagens tillämpningsområde ska inte heller omfatta behandling av personuppgifter inom personaladministration, asylärenden, invandring, gränskontroll eller bankernas behandling av personuppgifter. Behandlingsåtgärder som gäller sådana ärenden och situationer omfattas av tillämpningsområdet för allmänna dataskyddsförordningen.

Av de uppgifter som t.ex. Tullen ansvarar för enligt lag ska förhindrande och avslöjande av tullbrott samt förundersökning av tullbrott omfattas av dataskyddsdirektivets och den föreslagna lagens tillämpningsområde. Av de uppgifter som ålagts Tullen ska lagens tillämpningsområde inte omfatta uppgifter som t.ex. gäller verkställighet av EU:s tullagstiftning, verkställande av beskattning, tillsynsuppgifter, statistikföring av utrikeshandel eller laboratorieundersökningar. I fråga om dem blir allmänna dataskyddsförordningen tillämplig.

Enligt *2 mom. 1 punkten* ska lagen dessutom tillämpas på sådan behandling av personuppgifter som utförs av Försvarsmakten och för Försvarsmaktens räkning, när uppgifterna behandlas för skötsel av uppgifter som anges i 2 § 1 mom. 1 punkten, 2 punkten underpunkt a samt 3 och 4 punkten i lagen om försvarsmakten (551/2007). Sådan behandling av personuppgifter som avses i punkten faller inte under dataskyddsdirektivets tillämpningsområde. Det är alltså fråga om en utvidgning av tillämpningsområdet för den nationella lagen.

I 2 § 1 mom. 1 punkten i lagen om försvarsmakten föreskrivs om Försvarsmaktens huvuduppgift, som är det militära försvaret av Finland. Punkten delas upp på tre underpunkter, där det föreskrivs närmare om innehållet i uppgiften. I 2 § 1 mom. 1 punkten underpunkt a i lagen om försvarsmakten föreskrivs att till Försvarsmaktens uppgifter hör övervakning av Finlands landområden, vattenområden och luftrum samt tryggande av den territoriella integriteten.

Enligt 2 § 1 mom. 1 punkten underpunkt b i lagen om försvarsmakten hör det till skötseln av det militära försvaret av landet att trygga befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt att försvara den lagliga samhällsordningen. I 2 § 1 mom. 1 punkten underpunkt c i lagen föreskrivs att till Försvarsmaktens uppgifter hör att ge militärutbildning, styra den frivilliga försvarsutbildningen och stärka försvarsviljan.

Enligt 2 § 1 mom. 2 punkten i lagen om försvarsmakten hör stödjande av andra myndigheter till försvarsmaktens uppgifter. Uppgiften innefattar a) handräckning för upprätthållande av allmän ordning och säkerhet, för förhindrande och avbrytande av terroristbrott samt för skyddande av samhället i övrigt, samt b) deltagande i räddningsverksamheten genom att tillhandahålla utrustning, personalresurser och sakkunnigtjänster som behövs i räddningsverksamheten. Den föreslagna lagen ska tillämpas endast i samband med skötseln av uppgifter enligt underpunkt a.

Till Försvarsmaktens uppgifter hör enligt 2 § 1 mom. i den lagen för det tredje deltagande i stöd och bistånd som grundar sig på artikel 222 i fördraget om Europeiska unionens funktionssätt eller artikel 42.7 i fördraget om Europeiska unionen samt deltagande i territorialövervakningssamarbete eller i annat internationellt bistånd och annan internationell verksamhet. Till Försvarsmaktens fjärde uppgift hör enligt ovannämnda moment deltagande i internationell militär krishantering och i militäruppdrag i annan internationell krishantering. Närmare bestämmelser om deltagande i militär krishantering finns i lagen om militär krishantering.

Enligt 2 mom. *2 punkten* i den föreslagna paragrafen ska lagen tillämpas på sådan behandling av personuppgifter som utförs av polisen, när uppgifterna behandlas inom ramen för en i 1 § 1 mom. i polislagen avsedd uppgift som hänför sig till skyddet av den nationella säkerheten. Polisens uppgift är enligt 1 kap. 1 § 1 mom. i polislagen att trygga rätts- och samhällsordningen, upprätthålla allmän ordning och säkerhet samt att förebygga brott, avslöja och utreda brott och föra brott till åtalsprövning. I syfte att upprätthålla säkerheten samarbetar polisen med övriga myndigheter och sammanslutningar samt invånarna och sköter det internationella samarbete som deras uppgifter omfattar. Skyddspolisen har enligt 10 § i polisförvaltningslagen (110/1992) 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.

När skyddspolisen behandlar personuppgifter för att utföra sina ovannämnda uppgifter, dvs. för att skydda den nationella säkerheten, omfattas denna personuppgiftsbehandling inte av EU-rätten. Den nationella säkerheten har undantagits från EU:s behörighet i fördraget om Europeiska unionen. Därför ska bestämmelser om personuppgifter som behandlas på grundval av den nationella säkerheten utfärdas i den nationella lagstiftningen. Den föreslagna lagen ska tillämpas även på sådan behandling av personuppgifter som utförs av en annan polisenhet, när uppgifter behandlas i en i 1 § 1 mom. i polislagen avsedd uppgift som har samband med skyddet av den nationella säkerheten.

Enligt 2 mom. 3 punkten ska lagen tillämpas på sådan behandling av personuppgifter som utförs av Gränsbevakningsväsendet, när uppgifterna behandlas inom ramen för en i 3 § 2 och 3 mom. i gränsbevakningslagen avsedd uppgift som hänför sig till skyddet av den nationella säkerheten. I 3 § i gränsbevakningslagen föreskrivs om Gränsbevakningsväsendets uppgifter. Av dem hänför sig i synnerhet vissa tillsynsuppgifter och uppgifter inom det militära försvaret till skyddet av den nationella säkerheten. Enligt 3 § 2 mom. i gränsbevakningslagen utför gränsbevakningsväsendet tillsynsuppgifter som anges särskilt. Till dem hör bl.a. att övervaka och trygga Finlands territoriella integritet. Gränsbevakningsväsendet sörjer för territorialövervakningen i samarbete med Försvarsmakten och andra territorialövervakningsmyndigheter på det sätt som föreskrivs i territorialövervakningslagen. Enligt 3 § 3 mom. i gränsbevakningslagen deltar Gränsbevakningsväsendet i det militära försvaret. Enligt 25 § 1 mom. i gränsbevakningslagen ger Gränsbevakningsväsendet i detta syfte sin personal och de värnpliktiga som förordnats till Gränsbevakningsväsendet samt de kvinnor som antagits för att fullgöra frivillig militärtjänst militärutbildning samt upprätthåller och utvecklar försvarsberedskapen i samarbete med Försvarsmakten.

Enligt *3 mom.* ska 10 § 2 mom., 54 § och 7 kap. i den föreslagna lagen dock inte tillämpas på sådan behandling av personuppgifter som avses i 2 mom. I 10 § 2 mom. i den föreslagna lagen föreskrivs det om förutsättningarna för utlämnande av uppgifter till en mottagare inom EU, i 54 § om utlämnande av uppgifter till en tillsynsmyndighet i en annan EU-medlemsstat och i 7 kap. om överföringar av personuppgifter till tredjeländer. EU:s dataskyddslagstiftning gäller inte behandling av personuppgifter som sker på tillämpningsområdet för det föreslagna 2 mom., och de bestämmelser där som t.ex. gäller utlämnande av personuppgifter blir således inte tillämpliga.

Enligt *4 mom.* ska den föreslagna lagen dock tillämpas endast på sådan i 1 och 2 mom. avsedd behandling av personuppgifter som är helt eller delvis automatiserad eller där de uppgifter som behandlas utgör eller är avsedda att utgöra ett register eller en del av ett sådant. Lagens tillämpningsområde ska således också omfatta manuella register, och avsikten i förslaget är inte att till denna del ändra det rättsläge som anges i den gällande personuppgiftslagen. Enligt vad som konstateras i skäl 18 i ingressen i direktivet ska bestämmelserna inte gälla sådana akter eller grupper av akter som inte är ordnade enligt särskilda kriterier.

Paragrafens *5 mom.* innehåller en informativ bestämmelse om att dataskyddsdirektivet genomförs genom den föreslagna lagen.

2 §. *Förhållande till annan lagstiftning*. I *1 mom.* föreskrivs det för klarhets skull att om det i någon annan lag finns bestämmelser som avviker från den föreslagna lagen, ska de tillämpas i stället för denna lag. I praktiken finns det speciallagstiftning om nästan var och en av de behöriga myndigheter som avses i denna lag och den behandling av personuppgifter som de utför,

vilket innebär att de bestämmelserna ska tillämpas i stället för de bestämmelser som tas in i denna lag.

Paragrafens *2 mom.* innehåller en hänvisningsbestämmelse till lagstiftningen om offentlighet i myndigheternas verksamhet. Bestämmelser om rätten att ta del av myndigheternas offentliga handlingar finns särskilt i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt i lagen om offentlighet vid rättegång i allmänna domstolar (370/2007). De behöriga myndigheterna ska t.ex. vid utlämnande av personuppgifter ta hänsyn till offentlighetsprincipen och sekretessbestämmelserna på det sätt som föreskrivs i 12 § 2 mom. i grundlagen, i offentlighetslagen och i den speciallagstiftning som eventuellt blir tillämplig.

3 §. *Definitioner*. I paragrafen definieras de viktigaste begreppen i den föreslagna lagen. Paragrafen grundar sig på artikel 3 i dataskyddsdirektivet, med undantag för den definition av lämpliga skyddsåtgärder som avses i 1 mom. 10 punkten och den definition av tredjeland som avses i 15 punkten.

I 1 mom. *1* och *2 punkten* definieras personuppgifter, en registrerad och behandling av personuppgifter. Definitionernas innehåll ändras inte jämfört med gällande lagstiftning, men ordalydelsen uppdateras så att den bättre motsvarar definitionerna i dataskyddsdirektivet och i allmänna dataskyddsförordningen.

Med personuppgifter avses varje upplysning som direkt eller indirekt avser en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till ett namn, en personbeteckning eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, genetiska eller t.ex. sociala identitet. För att bedöma om en fysisk person är identifierbar bör man i enlighet med skäl 21 i ingressen i dataskyddsdirektivet beakta alla hjälpmedel, såsom utgallring, som, antingen av den personuppgiftsansvarige eller av någon annan aktör, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att bedöma om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva omständigheter, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Bestämmelserna om skydd för personuppgifter ska således inte tillämpas på anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, såsom statistik, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte längre är identifierbar.

Begreppet *begränsning av behandling* i *3 punkten* är nytt. Med begränsning av behandling avses markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.

Begreppet register, som finns i *4 punkten*, motsvarar innehållsmässigt till väsentliga delar begreppet personregister, vilket används för närvarande i personuppgiftslagen. Definitionen ändras så att den överensstämmer med definitionsbestämmelsen i dataskyddsdirektivet. Med register avses en strukturerad samling av personuppgifter som är tillgängliga enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

I *5 punkten* definieras *behörig myndighet*. Med behörig myndighet avses en myndighet som har behörighet att förebygga, avslöja, utreda brott eller föra brott till åtalsprövning, att åtalspröva eller vidta andra åtgärder som avser åtal för brott eller att döma till straffrättsliga påföljder eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten. Exempel på sådana behöriga myndigheter som avses i punkten är polis-

och tullmyndigheterna, Gränsbevakningsväsendet, de allmänna domstolarna, åklagarväsendet, Rättsregistercentralen samt Brottspåföljdsmyndigheten. Även en i lagen om Forststyrelsens jakt- och fiskeövervakning (1157/2005) avsedd jakt- och fiskeövervakare är en sådan behörig myndighet som avses i punkten, eftersom jakt- och fiskeövervakare i vissa situationer gör en summarisk förundersökning för att utreda ett brottmål. Likaså är t.ex. riksdagens justitieombudsman och justitiekanslern sådana behöriga myndigheter som avses i lagen, eftersom de i vissa situationer har åtalsrätt. Däremot är t.ex. en socialarbetare som fungerar som sådan biträdande övervakare som avses i lagen om verkställighet av samhällspåföljder (400/2015) och som utsetts att bistå en tjänsteman som svarar för verkställigheten av en enskild samhällspåföljd inte en sådan behörig myndighet som avses i punkten.

I punkten utsträcks definitionen av behörig myndighet till att också gälla Försvarsmakten, polisen och Gränsbevakningsväsendet när de sköter uppgifter som avses i det föreslagna 1 § 2 mom. Det är till denna del fråga om nationell reglering.

I *6 punkten* definieras *personuppgiftsansvarig*. Definitionen motsvarar i stor utsträckning nuläget. På lagens tillämpningsområde är den personuppgiftsansvarige alltid uttryckligen en behörig myndighet. Den personuppgiftsansvarige bestämmer ensam eller tillsammans med andra ändamålen och medlen för behandlingen av personuppgifter eller har enligt lag till uppgift att föra ett register. Bestämmelsen gör det således möjligt med gemensamt personuppgiftsansvariga på motsvarande sätt som för närvarande. Närmare bestämmelser om gemensamt personuppgiftsansvariga tas in i den föreslagna 16 §.

I *7 punkten* definieras *personuppgiftsbiträde*. Med personuppgiftsbiträde avses enligt förslaget en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. på basis av ett uppdragsförhållande. Med personuppgiftsbiträde avses således inte en person som är anställd hos den personuppgiftsansvarige, inte heller en enskild person som är anställd hos personuppgiftsbiträdet.

Definitionen i *8 punkten* är ny. Enligt den avses med *mottagare* en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ till vilket personuppgifterna lämnas ut.

I *9 punkten* definieras *personuppgiftsincident*. Den gällande personuppgiftslagen innehåller ingen definition av personuppgiftsincident. Med personuppgiftsincident avses enligt punkten en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Enligt definitionen förutsätter en personuppgiftsincident inte att incidenten har förorsakat den registrerade konkret skada.

I *10 punkten* definieras vad som i den föreslagna lagen avses med *lämpliga skyddsåtgärder*. Enligt punkten avses med lämpliga skyddsåtgärder sådana tekniska och organisatoriska åtgärder som säkerställer att behandlingen av personuppgifter är lagenlig, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerades rättigheter (riskbaserat förhållningssätt). Sådana åtgärder kan, beroende på fallet, bestå t.ex. av pseudonymisering eller hemlighållande av personuppgifter, införande av striktare förutsättningar för behandling av uppgifter än vad lagstiftningen förutsätter och utbildning i informationssäkerhetsfrågor för den personal som behandlar uppgifter. Skyddsåtgärderna kan också omfatta fullgörande av i lag eller förordning angivna informationssäkerhetsskyldigheter som är exaktare än de skyldigheter som ingår i denna lag. Det är inte möjligt att på ett uttömmande sätt definiera lämpliga skyddsåtgärder i lagen, och arten av de skyddsåtgärder som krävs kan med tiden förändras, bl.a. på grund av den tekniska utvecklingen. En motsvarande definition

finns inte uttryckligen i dataskyddsdirektivet. I den föreslagna lagen hänvisas det på flera ställen till lämpliga skyddsåtgärder.

I *11 punkten* definieras vad som i lagen avses med *profilering.* Med profilering avses automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person. Profileringen görs vanligen i syfte att analysera eller förutsäga aspekter rörande denna fysiska persons intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

I *12 punkten* definieras *genetiska uppgifter* som personuppgifter som rör sådana nedärvda eller förvärvade genetiska kännetecken för en fysisk person som ger unik information om personens fysiologi eller hälsa, och som härrör från en analys av ett biologiskt prov från personen i fråga eller som erhållits på annat sätt. Definitionen är ny.

I *13 punkten* definieras *biometriska uppgifter*. Någon motsvarande definition ingår inte i den gällande lagstiftningen om personuppgifter. Med biometriska uppgifter avses personuppgifter som tagits fram genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av personen i fråga. Biometriska uppgifter är t.ex. ansiktsbilder och fingeravtrycksuppgifter.

Definitionen *av uppgifter om hälsa* i *14 punkten* är ny. Med uppgifter om hälsa avses personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa och som ger information om personens hälsotillstånd. Definitionen omfattar alla uppgifter som gäller den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Med uppgifter om hälsa avses bl.a. genetiska och biologiska uppgifter samt uppgifter om sjukdom, funktionshinder, sjukdomsrisk och klinisk behandling.

I *15 punkten* definieras *tredjeland*. Med tredjeland avses andra stater än medlemsstater i Europeiska unionen (EU), stater inom Europeiska ekonomiska samarbetsområdet eller Schweiz. Till Europeiska ekonomiska samarbetsområdet hör utöver EU:s medlemsstater Island, Liechtenstein och Norge.

I *16 punkten* definieras vad som i den föreslagna lagen avses med *internationell organisation*. Med begreppet avses en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som har inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater. En sådan internationell organisation som avses i punkten är t.ex. Interpol.

Enligt *2 mom.* ska vad som i den föreslagna lagen föreskrivs om behörig myndighet tillämpas också på enskilda som sköter en uppgift som avses i 1 mom. 5 punkten. Bestämmelsen grundar sig på artikel 3.7 b i dataskyddsdirektivet. Enligt artikeln avses med behörig myndighet också ett annat organ eller en annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. De bestämmelser som föreslås i momentet behövs för att enskilda aktörer som sköter sådana uppgifter i andra EU-länder, såsom organisationer som upprätthåller privata fängelser, ska beaktas.

Enligt *3 mom.* ska vad som i den föreslagna lagen föreskrivs om en medlemsstat i EU tillämpas också på stater inom Europeiska ekonomiska samarbetsområdet och på Schweiz. Förslaget grundar sig på bestämmelserna i direktivet. Till Europeiska ekonomiska samarbetsområdet hör för närvarande utöver EU:s medlemsstater Island, Liechtenstein och Norge.

2 kap. Principer för behandling av personuppgifter

Kapitlet innehåller bestämmelser om principerna för behandling av personuppgifter. De ska iakttas alltid när personuppgifter behandlas i enlighet med den föreslagna lagen.

4 §. *Krav på laglig behandling*. Paragrafen innehåller bestämmelser om krav på laglig behandling av personuppgifter. Den föreslagna paragrafen grundar sig på artikel 4.1 a och b samt artikel 8.1 i dataskyddsdirektivet. Paragrafen motsvarar i huvuddrag 5 § i personuppgiftslagen, där det föreskrivs om aktsamhetsplikt, samt 8 § 4 punkten och 12 § 5 punkten i den lagen. Enligt 5 § i personuppgiftslagen ska den registeransvarige behandla personuppgifterna i enlighet med lag och vid behandlingen iaktta aktsamhet och god informationshantering och även i övrigt förfara så att skyddet av den registrerade privatliv och andra grundläggande fri- och rättigheter som tryggar skyddet för den personliga integriteten inte begränsas utan en i lag angiven grund.

Enligt *1 mom.* får personuppgifter behandlas endast om det behövs för att en behörig myndighet ska kunna utföra en i lag angiven uppgift på ett område som anges i 1 § 1 och 2 mom. Med lag avses i detta sammanhang både inhemsk lag och EU-lagstiftning.

Behandlingen ska behövas för att en behörig myndighet ska kunna utföra en uppgift som avses i 1 § 1 eller 2 mom. I enlighet med relevans- och proportionalitetskraven bör personuppgifter behandlas endast i en sådan omfattning att ändamålet med behandlingen inte rimligen kan uppnås genom andra medel.

Enligt *2 mom.* ska personuppgifter behandlas på ett korrekt och omsorgsfullt sätt. Dessa krav hänvisar för sin del bl.a. till kraven på informationssäkerhet, och av dem följer också en mer allmän skyldighet att behandla personuppgifter i enlighet med god informationshantering. Aktsamhetsplikten framhäver på motsvarande sätt som i 5 § i den gällande personuppgiftslagen att den personuppgiftsansvariges tar egna initiativ för att säkerställa att de bestämmelser och principer som gäller skydd för personuppgifter iakttas vid behandlingen av personuppgifter.

5 §. *Ändamålsbegränsning*. Paragrafen innehåller bestämmelser om principen om ändamålsbegränsning. Genom paragrafen genomförs artikel 4.1 b, 4.2 och 4.3 samt artikel 9. En bestämmelse om ändamålsbundenhet ingår i 7 § i personuppgiftslagen.

Enligt *1 mom.* i den föreslagna paragrafen får den personuppgiftsansvarige samla in personuppgifter endast för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandla dem på ett sätt som står i strid med dessa ändamål.

Enligt *2 mom.* får personuppgifter som har samlats in för ett ändamål som anges i 1 § 1 eller 2 mom. i den föreslagna lagen behandlas för något annat än ett i momentet angivet ändamål endast om det föreskrivs om behandlingen i lag. Dessa bestämmelser riktar sig till såväl den ursprungliga personuppgiftsansvarige som andra personuppgiftsansvariga. Kravet på laglighet kan uppfyllas genom såväl nationell lagstiftning som unionslagstiftning. En sådan lag ska uppfylla kraven i dataskyddsdirektivet på nödvändig och proportionell behandling på det sätt som förutsätts i artikel 4.2 b i direktivet. Om personuppgifter behandlas för de andra ändamål till vilka det hänvisas i bestämmelsen, tillämpas i princip allmänna dataskyddsförordningen på behandlingen.

Enligt *3 mom.* får personuppgifter behandlas i ett i 1 § 1 eller 2 mom. angivet syfte också för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål. En förutsättning då är emellertid att lämpliga skyddsåtgärder för de registrerades rättigheter har vidtagits. Till den del den behandling som avses i momentet sker för några andra än i 1 §

angivna ändamål, tillämpas allmänna dataskyddsförordningen, den föreslagna dataskyddslagen samt eventuell speciallagstiftning om behandling av personuppgifter.

Den personuppgiftsansvarige ska kunna visa att denne har iakttagit bestämmelserna i den föreslagna paragrafen.

6 §. *Relevanskrav*. Genom den föreslagna paragrafen genomförs artikel 4.1 c och e samt artikel 5 i dataskyddsdirektivet. Paragrafen innehåller bestämmelser om relevanskrav och begränsningar i bevarandet av uppgifter, något som i väsentlig grad har samband med relevanskravet. Tillsammans tillgodoser bestämmelserna principen om minimering av uppgifter. Bestämmelser om relevanskrav finns för närvarande i 9 § 1 punkten i personuppgiftslagen.

Enligt *1 mom.* ska de personuppgifter som behandlas vara adekvata och behövliga med hänsyn till ändamålet med behandlingen och får inte vara för omfattande i förhållande till de ändamål för vilka de behandlas. Obehövliga personuppgifter ska utplånas utan obefogat dröjsmål. Den personuppgiftsansvarige ska vid behov kunna visa att behandlingen behövs.

Enligt *2 mom.* får personuppgifter inte lagras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som behövs (i direktivets svenska version används *är nödvändigt*) med hänsyn till ändamålet med behandlingen.

Enligt artikel 5 i dataskyddsdirektivet ska medlemsstaterna föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Enligt 3 mom. ska behovet att bevara personuppgifter bedömas med minst fem års mellanrum, om inte något annat föreskrivs om bevaringstider för personuppgifter någon annanstans. Genom momentet säkerställs att behovet att bevara personuppgifterna bedöms regelbundet också i det fall att det i speciallagstiftning saknas särskilda bestämmelser om bedömning av behovet av bevarande. Den personuppgiftsansvarige ska med beaktande av de skyldigheter som tas in i den föreslagna 14 § genomföra åtgärder för att säkerställa att bevaringstiden iakttas. I enlighet med vad som föreskrivs i 12 § 2 mom. i den gällande personuppgiftslagen ska behovet att bevara uppgifter om brott och påföljder för brott också för närvarande i princip bedömas minst vart femte år.

7 §. *Felfrihetskrav*. Paragrafen innehåller bestämmelser om felfrihetskrav, vilket är en av principerna för behandling av personuppgifter. Genom paragrafen genomförs den bestämmelse om att föreskriva om saken i lag som ingår i artikel 4.1 d i dataskyddsdirektivet. En bestämmelse om felfrihetskrav ingår i 9 § 2 mom. i personuppgiftslagen. Även om den grundläggande utgångspunkten för kravet kvarstår oförändrat, ses ordalydelsen i bestämmelsen över i förhållande till personuppgiftslagen så att den motsvarar dataskyddsdirektivet.

Enligt paragrafen ska de personuppgifter som behandlas vara korrekta och vara uppdaterade med hänsyn till ändamålet med behandlingen. Kravet innebär i praktiken t.ex. att personuppgifter med ett vagt innehåll i princip inte ska behandlas. Bestämmelsen utgör i sig inget hinder för att sådana uppgifter lagras vars sanningsenlighet inte omedelbart kan verifieras eller där det är fråga t.ex. om ett vittnes subjektiva åsikter. Den personuppgiftsansvarige ska vidta alla rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas antingen utplånas eller rättas utan dröjsmål. De behöriga myndigheterna bör likaså säkerställa att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga eller överhuvudtaget samlas in. Vid tillämpningen av den uppdateringsskyldighet som avses i paragrafen ska det tas hänsyn till ändamålet med behandlingen av personuppgifterna samt vilken betydelse behandlingen har med tanke på den registrerades integritetsskydd och rättssäkerhet.

8 §. *Åtskillnad mellan olika personuppgifter*. I paragrafen föreskrivs det om en skyldighet att skilja vissa personuppgifter från varandra. Paragrafen grundar sig på artikel 6 och 7.1 i dataskyddsdirektivet. Någon motsvarande bestämmelse finns inte i personuppgiftslagen. Den föreslagna bestämmelsen har dock en nära koppling t.ex. till det felfrihetskrav om vilket det föreskrivs i 7 § i den föreslagna lagen.

Enligt *1 mom.* ska den personuppgiftsansvarige vid behov och så långt det är möjligt göra en klar åtskillnad mellan personuppgifter som avser registrerade i olika ställning med tanke på det ärende som behandlas. Alla rimliga åtgärder med beaktande av vikten av åtskillnad ska vidtas för att skilja uppgifterna åt. Om en persons ställning entydigt framgår av sammanhanget, behövs i princip inga åtgärder för att göra åtskillnad mellan uppgifterna.

Personer som kan anses stå i olika ställning i förhållande till varandra är t.ex. personer för det vilka det finns skäl att misstänka att de har begått eller är på väg att begå ett brott samt personer som har dömts för brott.

Enligt *2 mom.* ska alla rimliga åtgärder vidtas för att skilja personuppgifter som grundar sig på fakta från personuppgifter som grundar sig på personliga bedömningar. Under förundersökningen t.ex. ges det ofta utlåtanden som innehåller personuppgifter, men som grundar sig på fysiska personers subjektiva iakttagelser. Sådana uppgifter kan inte alltid verifieras och ska i princip hållas åtskilda från personuppgifter som grundar sig på fakta. Exempel på uppgifter som baserar sig på fakta är teleövervakningsuppgifter som visar på kontakt med en annan person.

9 §. *Säkerställande av kvaliteten på personuppgifter som överförs eller görs tillgängliga*. Paragrafen innehåller krav när det gäller att säkerställa kvaliteten på personuppgifter om överförs eller görs tillgängliga. Med överföring avses såväl teknisk överföring som egentligt utlämnande av personuppgifter. I paragrafen framhävs särskilt aktsamhets- och felfrihetskravet i samband med att personuppgifter överförs eller görs tillgängliga. Genom paragrafen genomförs artikel 7.2 och 7.3 i dataskyddsdirektivet.

Enligt *1 mom.* ska den behöriga myndigheten vidta alla rimliga åtgärder för att se till att personuppgifter som är oriktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska därför så långt det är möjligt kontrollera kvaliteten på personuppgifterna alltid innan dessa överförs eller görs tillgängliga. Sådana åtgärder som skulle medföra en oskälig administrativ börda i förhållande till syftet med överföringen förutsätts inte.

Enligt *2 mom.* ska, vid all överföring av personuppgifter, så långt det är möjligt, sådan information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga, tillförlitliga och aktuella.

Om det visar sig att oriktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts, ska mottagaren enligt vad som föreslås i 3 mom. utan dröjsmål informeras om detta. Efter att mottagaren informerats om saken ska denne rätta eller utplåna de erhållna personuppgifterna eller begränsa behandlingen av dem. Begreppet mottagare definieras i 3 § 1 mom. 8 punkten. Även den behöriga myndighet som överfört personuppgifterna ska vidta lämpliga åtgärder, såsom att rätta felaktiga personuppgifter som myndigheten innehar.

10 §. *Skyldighet att informera om särskilda förutsättningar för behandlingen*. Paragrafen innehåller bestämmelser om en skyldighet för den behöriga myndigheten att informera om särskilda förutsättningar för behandlingen i enlighet med artikel 9.3 och 9.4 i dataskyddsdirektivet.

I *1 mom.* föreskrivs att om det i lag anges särskilda förutsättningar för behandling av personuppgifter, ska den behöriga myndigheten i samband med utlämnande eller överföring av personuppgifter informera mottagaren av personuppgifterna om dessa förutsättningar samt om skyldigheten att iaktta dem. Sådana förutsättningar kan till exempel innefatta ett förbud mot att överföra personuppgifter till andra eller använda dem i andra syften än de för vilka de har överförts till mottagaren. Sådana särskilda förutsättningar kan också innefatta ett förbud mot att informera den registrerade om en begränsning av rätten till information utan förhandsgodkännande från den överförande behöriga myndigheten. Bestämmelser om sådana särskilda förutsättningar kan tas in i den speciallagstiftning som tillämpas på de behöriga myndigheterna.

Enligt *2 mom.* får den behöriga myndigheten när den överför personuppgifter till en mottagare inom EU inte uppställa strängare krav på behandlingen av personuppgiften än vad som tillämpas nationellt på likartade uppgiftsöverföringar.

11 §. *Behandling av särskilda kategorier av personuppgifter*. I paragrafen föreskrivs det om särskilda kategorier av personuppgifter och behandlingen av dem. Bestämmelsen grundar sig på artikel 10 i dataskyddsdirektivet.

Bestämmelser om uppgifter om hör till särskilda kategorier av personuppgifter tas in i *1 mom*. Definitionen av särskilda kategorier av personuppgifter skiljer sig till vissa delar från motsvarande definition i 11 § i personuppgiftslagen. Särskilda kategorier av personuppgifter ska inte heller längre kallas känsliga uppgifter. Uppgifter som hör till särskilda kategorier av personuppgifter är personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Till särskilda kategorier av personuppgifter hör också genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person, såsom fingeravtrycksuppgifter och ansiktsbilder, samt uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Etniskt ursprung inbegriper också ”ras” i enlighet med artikel 10 i dataskyddsdirektivet.

Det är i princip förbjudet att behandla särskilda kategorier av personuppgifter. Behandling av sådana uppgifter är tillåten endast i de situationer som räknas upp i *2 mom*. Enligt den föreslagna bestämmelsen är sådan behandling tillåten, om det är nödvändigt och de skyddsåtgärder som krävs för att trygga den registrerades rättigheter har vidtagits. På grund av kravet på nödvändighet får uppgifter som hör till särskilda kategorier av uppgifter inte behandlas, om målet med behandlingen kan uppnås på något annat sätt som ingriper mindre i den registrerades rättigheter. En ytterligare förutsättning är att det föreskrivs om behandlingen i lag, att det är fråga om handläggning av brottmål i åklagarverksamhet eller i domstol eller att behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade eller att det krävs för att skydda ett intresse som är av grundläggande betydelse för den registrerade eller en annan fysisk person. Enligt skäl 37 i ingressen i dataskyddsdirektivet kan de lämpliga skyddsåtgärder som krävs vid behandling av uppgifter som hör till särskilda kategorier av personuppgifter t.ex. inbegripa möjligheten att samla in dessa uppgifter endast i samband med andra uppgifter om den berörda fysiska personen, möjligheten att säkra de insamlande uppgifterna, striktare regler om tillgång till uppgifterna för den behöriga myndighetens personal på lämpligt sätt och förbud mot att översända sådana uppgifter.

I paragrafens *3 mom.* föreslås en bestämmelse om profilering. Enligt vad som föreskrivs i artikel 11 i dataskyddsdirektivet är profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter förbjuden. Med profilering avses enligt den definition som föreslås i 3 § 1 mom. 11 punkten automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma personliga egenskaper hos en fysisk person, såsom pålitlighet, beteende, intressen eller förflyttningar. Med diskrimine-

ring åter avses att utan godtagbart skäl särbehandla en person av en orsak som avses i 1 mom., enligt vad som föreskrivs om detta bl.a. i artikel 21 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna samt i 6 § 2 mom. i grundlagen. I praktiken förbjuds genom bestämmelsen i princip t.ex. en sådan på algoritmer baserad profilering som leder till att personer som hör till en viss etnisk grupp blir föremål för striktare övervakning eller kontroll än andra.

12 §. *Behandling av personbeteckningar*. I paragrafen föreslås bestämmelser om behandling av personbeteckningar. Dataskyddsdirektivet innehåller inga uttryckliga bestämmelser om behandling av personbeteckningar. De föreslagna bestämmelserna är således enbart nationella. Bestämmelser om behandling av personbeteckning finns också i 29 § i personuppgiftslagen.

Bestämmelser om de särskilda förutsättningar som gäller för behandling av personbeteckningar tas in i *1 mom.* Enligt det föreslagna momentet får en personbeteckning behandlas endast om det är viktigt att entydigt identifiera den registrerade för att en behörig myndighet ska kunna utföra en i lag angiven uppgift eller för att tillgodose den registrerades eller den personuppgiftsansvariges rättigheter eller uppfylla den registrerades eller den personuppgiftsansvariges skyldigheter. En personbeteckning får behandlas också om det är viktigt att entydigt identifiera den registrerade för sådan historisk eller vetenskaplig forskning eller sådan statistikföring som avses i 5 § 3 mom. i den föreslagna lagen.

Enligt det föreslagna *2 mom.* får en personbeteckning inte onödigtvis antecknas i handlingar som skrivs ut eller upprättas på basis av ett register. Förslaget motsvarar 13 § 4 mom. i personuppgiftslagen.

13 §. *Automatiserat individuellt beslutsfattande*. Paragrafen innehåller bestämmelser om automatiserat individuellt beslutsfattande. En bestämmelse om detta finns i artikel 11 i dataskyddsdirektivet. I 31 § i personuppgiftslagen finns en bestämmelse, med något annorlunda innehåll, om automatiserade beslut.

Enligt den föreslagna paragrafen är ett beslut som fattas enbart på grundval av automatiserad behandling av personuppgifter och som har negativa rättsverkningar för den registrerade eller annars är betydande för denne förbjudna. Sådant automatiserat individuellt beslutsfattande är enligt den föreslagna bestämmelsen tillåtet endast om så föreskrivs någon annanstans i lag. I praktiken ska sådant automatiserat beslutsfattande således alltid regleras i speciallagstiftning. Sådan lagstiftning ska uppfylla kraven i artikel 11 i direktivet bl.a. när det gäller den registrerades rätt att kräva att en fysisk person från den personuppgiftsansvariges sida deltar i behandlingen.

Paragrafen ska gälla situationer då beslutsfattandet grundar sig enbart på automatiserad behandling av personuppgifter, dvs. då ingen fysisk person deltar i beslutsfattandet. Den blir således tillämplig i sådana situationer då t.ex. en person som är anställd hos den personuppgiftsansvarige deltar i behandlingen av personuppgifter endast på ett sådant sätt som inte har någon inverkan på beslutsfattandet. Sådana i paragrafen avsedda mekanismer för beslutsfattande som grundar sig enbart på automatiserad behandling av personuppgifter används veterligen inte på den föreslagna lagens tillämpningsområde i Finland för närvarande.

3 kap. Personuppgiftsansvarig och personuppgiftsbiträde

14 §. *Den personuppgiftsansvariges ansvar*. Paragrafen innehåller bestämmelser om ansvaret för den personuppgiftsansvariga som avses i den föreslagna lagen. De föreslagna bestämmelserna grundar sig på artikel 19.1 i dataskyddsdirektivet.

Enligt *1 mom.* svarar den personuppgiftsansvarige för att personuppgifter behandlas i enlighet med lag. Den personuppgiftsansvarige ska realisera sitt ansvar genom anvisningar till sina anställda eller personuppgiftsbiträdet samt efter behov t.ex. genom utbildning. Bestämmelser om vilka tekniska och organisatoriska åtgärder som krävs av den personuppgiftsansvarige tas in i 2 mom. Den personuppgiftsansvarige påförs också en s.k. ansvarsskyldighet, dvs. den personuppgiftsansvarige ska också i efterskott kunna visa att personuppgifterna har behandlats i enlighet med de principer som anges i lagens 2 kap.

Enligt *2 mom.* är den personuppgiftsansvarige skyldig att vidta de tekniska och organisatoriska åtgärder som krävs med avseende på ansvaret enligt 1 mom. för att den personuppgiftsansvarige ska kunna säkerställa och även visa att behandlingen av personuppgifter är laglig. När åtgärderna vidtas ska det enligt den föreslagna bestämmelsen tas hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter. När åtgärderna planeras ska det således t.ex. tas hänsyn till huruvida de personuppgifter som behandlas gäller personer i en ytterst utsatt position, såsom barn eller offer för människohandel. Det kan också vara av betydelse om behandlingen gäller en stor mängd personuppgifter eller uppgifter som hör till särskilda kategorier av personuppgifter. I sådana situationer ska särskilda skyddsåtgärder planeras och vidtas.

15 §. *Inbyggt dataskydd och dataskydd som standard*. Paragrafen innehåller bestämmelser om inbyggt dataskydd och dataskydd som standard (*privacy by design ja privacy by default*). Genom den genomförs artikel 20 i dataskyddsdirektivet. Det är fråga om en ny typ av skyldighet jämfört med personuppgiftslagen.

Enligt *1 mom.* ska den personuppgiftsansvarige redan vid tidpunkten för beslut om hur behandlingen av personuppgifter ska utföras och vid tidpunkten för själva behandlingen av personuppgifter genomföra lämpliga tekniska och organisatoriska skyddsåtgärder för att säkerställa att behandlingen är laglig och att den registrerades rättigheter skyddas. Åtgärderna ska vidtas med beaktande av tillgängliga tekniska lösningar, genomförandekostnaderna samt behandlingens art, omfattning, sammanhang och ändamål samt de risker som behandlingen medför för personens rättigheter. De åtgärder som avses i momentet kan t.ex. bestå av pseudonymisering så snart det är möjligt med tanke på ändamålet med behandlingen. De krav som uppställs i momentet ska beaktas också t.ex. när informationssystem genomförs.

Riskens sannolikhetsgrad och allvar bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken ska bedömas utifrån objektiva omständigheter. Det kan anses vara fråga om en betydande risk i synnerhet när det finns risk för att de registrerades rättigheter försämras. Behandling t.ex. av uppgifter som hör till särskilda kategorier av personuppgifter eller av uppgifter som gäller särskilt utsatta kategorier av personer medför ofta en större risk för personens rättigheter, och i princip bör det då ställas högre krav på åtgärderna. Å andra sidan kan det också vara mycket riskfyllt att lämna ut eller göra uppgifterna tillgängliga som behandlingstyper.

Enligt *2 mom.* ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att i standardfallet säkerställa att endast personuppgifter som behövs (i direktivets svenska version används *är nödvändiga*) för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten ska gälla såväl mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring som deras tillgänglighet. Genom lämpliga åtgärder ska det särskilt säkerställas att personuppgifter i standardfallet inte görs tillgängliga för ett obegränsat antal fysiska personer utan den berörda personens medverkan.

16 §. *Gemensamt personuppgiftsansvariga*. Paragrafen innehåller bestämmelser om särskilda krav i situationer med gemensamt personuppgiftsansvariga. Bestämmelsen grundar sig på ar-

tikel 21 i dataskyddsdirektivet. Fler personuppgiftsansvariga är möjliga även med stöd av personuppgiftslagen, men den innehåller dock ingen sådan bestämmelse som den föreslagna paragrafen, genom vilken de inbördes förhållandena mellan gemensamt personuppgiftsansvariga preciseras.

Om två eller flera personuppgiftsansvariga gemensamt fastställer behandlingens ändamål och medel, ska de enligt *1 mom.* komma överens om den inbördes ansvarsfördelningen vid skötseln av skyldigheter enligt den föreslagna lagen, om det inte föreskrivs om ansvarsfördelningen i lag. När den inbördes ansvarsfördelningen fastställs gäller det att noggrant se till att lagens krav till alla delar beaktas. Även om de viktigaste uppgifterna i fråga om ansvarsfördelning och skyldigheter även i framtiden i stor utsträckning regleras i lag, medför den föreslagna bestämmelsen flexibilitet i arbetsfördelningen mellan de personuppgiftsansvariga.

Enligt *2 mom.* ska personuppgiftsansvariga som avses i 1 mom. inom sig utse en personuppgiftsansvarig som fungerar som kontaktpunkt. Med en personuppgiftsansvarig som fungerar som kontaktpunkt kan den registrerade i första hand ha kontakt i frågor som gäller utövandet av den registrerades rättigheter. I momentet föreskrivs det vidare att den registrerade dock alltid får utöva sina rättigheter enligt den föreslagna lagen i förhållande till var och en av de personuppgiftsansvariga.

17 §. *Personuppgiftsbiträde*. Paragrafen innehåller bestämmelser om personuppgiftsbiträde på det sätt som förutsätts i artikel 22.1, 22.2, 22.3 och 22.4 i dataskyddsdirektivet. Enligt 3 § 1 mom. 7 punkten i den föreslagna lagen avses med personuppgiftsbiträde en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Enligt *1 mom.* ska den som behandlar personuppgifter för den personuppgiftsansvariges räkning lämna den personuppgiftsansvarige lämpliga utredningar och förbindelser och även i övrigt tillräckliga garantier för de organisatoriska och tekniska åtgärder genom vilka det säkerställs att personuppgifterna behandlas i enlighet med kraven i den föreslagna lagen. En liknande bestämmelse ingår i 32 § 2 mom. i personuppgiftslagen. Enligt den föreslagna bestämmelsen bör också personuppgiftsbiträdet beakta exempelvis principen om inbyggt dataskydd och dataskydd som standard. De utredningar och förbindelse som avses i momentet kan tas in också i det avtal mellan den personregisteransvarige och personuppgiftsbiträdet som avses i 3 mom.

Paragrafens *2 mom.* innehåller ett förbud enligt vilket personuppgiftsbiträdet och en anställd hos personuppgiftsbiträdet inte får behandla personuppgifter på ett sätt som avviker från den personuppgiftsansvariges instruktioner. Om personuppgiftsbiträdet trots detta fastställer behandlingens ändamål och medel, betraktas personuppgiftsbiträdet som personuppgiftsansvarig i fråga om denna lagstridiga behandling. Personuppgiftsbiträdet får enligt den föreslagna bestämmelsen inte heller överföra behandlingen av personuppgifter på något annat personuppgiftsbiträde utan skriftligt tillstånd av den personuppgiftsansvarige. Den personuppgiftsansvarige kan ge ett sådant samtycke antingen för ett bestämt fall eller allmänt. Om den personuppgiftsansvarige ger ett allmänt samtycke till överföringen, ska personuppgiftsbiträdet dock informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden. Den personuppgiftsansvarige har med stöd av den föreslagna bestämmelsen rätt att förbjuda sådana ändringar.

Den behandling av personuppgifter som personuppgiftsbiträdet utför ska enligt *3 mom.* regleras i ett skriftligt avtal eller i ett skriftligt förordnande. Ett förordnande blir aktuellt närmast när en högre myndighet fungerar som personuppgiftsansvarig och en myndighet på samma förvaltningsområde är personuppgiftsbiträde. Avtalet eller förordnandet kan också finnas i

elektronisk form. Av handlingen ska framgå typen av personuppgifter, behandlingens varaktighet, art och ändamål, kategorierna av personuppgifter och kategorierna av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter. Skyldigheten att upprätta ett avtal eller någon annan handling gäller också sådana situationer då personuppgiftsbiträdet överför behandlingen till ett annat personuppgiftsbiträde. Då måste ett avtal upprättas också mellan dem.

I det avtal eller förordnande som avses i det föreslagna 3 mom. ska dessutom uttryckligen bestämmas att personuppgiftsbiträdet ska handla enbart enligt instruktioner från den personuppgiftsansvarige. Dessutom ska det bestämmas eller avtalas om att personuppgiftsbiträdet ska säkerställa att de fysiska personer som behandlar personuppgifterna har förbundit sig att iaktta sekretess eller att de omfattas av en lagstadgad tystnadsplikt. Personuppgiftsbiträdet ska på lämpligt sätt bistå den personuppgiftsansvarige för att säkerställa att de bestämmelser som gäller den registrerades rättigheter iakttas.

Av handlingen ska det också framgå att personuppgiftsbiträdet, beroende på den personuppgiftsansvariges val, ska utplåna eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och utplåna befintliga kopior, om inte något annat föreskrivs i lag. I handlingen ska det också nämnas att personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som behövs (i direktivets svenska version används krävs) för att visa att den föreslagna paragrafen iakttas samt uppfylla de förutsättningar som avses i paragrafen för anlitande av ett annat personuppgiftsbiträde.

18 §. *Register över behandlingar*. Paragrafen grundar sig på artikel 24 i dataskyddsdirektivet. Här åläggs både den personuppgiftsansvarige och personuppgiftsbiträdet att föra ett register över behandlingen. De register som avses i paragrafen ska vara skriftliga, och de kan också upprättas i elektronisk form. Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra registren tillgängliga för tillsynsmyndigheten på grundval av myndighetens rätt till information. De föreslagna bestämmelserna skiljer sig från den registerbeskrivning som anges i 10 § i personuppgiftslagen, eftersom det register som anges i den föreslagna lagen inte behöver hållas allmänt tillgängligt.

I *1 mom.* föreskrivs det om den personuppgiftsansvariges register över behandlingen. Enligt momentet ska den personuppgiftsansvarige föra ett skriftligt register över behandling av personuppgifter som utförts under dess ansvar. Registret ska innehålla åtminstone de uppgifter som uppräknas i registret. Utöver obligatoriska uppgifter kan det ibland finnas behov att i registret redogöra också för andra omständigheter som är viktiga att delge den registrerade eller utomstående. Mängden obligatoriska uppgifter är mer omfattande än vad som förutsätts i 10 § i personuppgiftslagen. Nya krav är t.ex. att det ska antecknas huruvida profilering används samt de planerade tidsfristerna för utplåning av olika kategorier av personuppgifter. En definition av profilering tas in i 3 § 1 mom. 11 punkten i den föreslagna lagen. Om personuppgifter överförs till ett tredjeland eller en internationell organisation, ska det av registret framgå vilket tredjeland eller vilken internationell organisation det är fråga om.

Enligt *2 mom.* ska personuppgiftsbiträdet föra ett skriftligt register över all behandling av personuppgifter som utförs för den personuppgiftsansvariges räkning. Någon motsvarande skyldighet finns inte i den gällande personuppgiftslagen. Det register som personuppgiftsbiträdet för ska för det första innehålla uppgifter om personuppgiftsbiträdet och dataskyddsombudet samt deras kontaktuppgifter. Registret ska dessutom uppta alla de personuppgiftsansvariga för vars räkning personuppgiftsbiträdet agerar samt deras namn och kontaktuppgifter liksom de kategorier av behandling som har utförts för vare personuppgiftsansvarigs räkning. Dessutom ska registret innehålla eventuella uppgifter om överföringar av personuppgifter till ett tredje-

land eller en internationell organisation, om den personuppgiftsansvarige uttryckligen begär detta. Om möjligt ska registret också innehålla en allmän beskrivning av de tekniska och organisatoriska skyddsåtgärder som avses i 31 § i den föreslagna lagen.

19 §. *Logguppgifter*. Paragrafen innehåller bestämmelser om en skyldighet att samla in och bevara logguppgifter. Genom paragrafen genomförs den bestämmelse om att föreskriva om saken i lag som ingår i artikel 25 i dataskyddsdirektivet. Någon motsvarande skyldighet att föra loggar finns inte i personuppgiftslagen, men i speciallagstiftning, såsom i polisens personuppgiftslag, ingår skyldigheten även för närvarande.

Även logguppgifter ska betraktas som personuppgifter. De är personuppgifter om de personer som använder informationssystemen. Eftersom andra personer inte är sådana registrerade som avses här, har de i princip inte sådan rätt till insyn i fråga om de i paragrafen avsedda logguppgifterna som föreslås bli föreskrivet. Det kan dock bli aktuellt att få uppgifter ur myndighetens loggar, om en person har rätt att få uppgifterna i fråga ur loggarna med stöd av 11 § i offentlighetslagen, eftersom dessa loggar ska betraktas som myndighetshandlingar. Även dataombudsmannen ska med stöd av sin rätt till information ha rätt att få uppgifter ur loggarna.

Enligt *1 mom.* ska den personuppgiftsansvarige och personuppgiftsbiträdet se till att logguppgifter bevaras över insamling, ändring, läsning, utlämnande, överföring, sammanförande och utplåning av personuppgifter som utförts i deras automatiserade behandlingssystem. En ytterligare förutsättning är att de logguppgifter som gäller läsning och utlämnande ska göra det möjligt att utreda grund, datum och tidpunkt för läsning och utlämnande och i möjligaste mån vem som har läst eller lämnat ut personuppgifterna samt mottagarnas identitet. Grunden för läsningen eller utlämnandet behöver således inte nödvändigtvis framgå direkt av logguppgifterna, men dessa omständigheter ska enligt de föreslagna bestämmelserna kunna utredas utifrån logguppgifterna. Av bestämmelsen följer att också utlämnande som skett t.ex. per telefon eller e-post ska ge upphov till en anteckning, av vilken de uppgifter som uppräknas i bestämmelsen framgår.

I *2 mom.* föreskrivs det om för vilka ändamål logguppgifterna får användas. Förteckningen i momentet är uttömmande. Logguppgifterna får användas endast för att kontrollera om behandlingen är lagenlig, för att säkerställa personuppgifternas integritet och säkerhet, inom ramen för straffrättsliga förfaranden samt för intern kontroll. Intern kontroll kan även omfatta behöriga myndigheters interna disciplinära förfaranden.

20 §. *Konsekvensbedömning avseende dataskydd*. I paragrafen föreskrivs det om den personuppgiftsansvariges skyldighet att göra en konsekvensbedömning avseende dataskydd. Någon motsvarande bestämmelse finns inte i personuppgiftslagen. Bestämmelsen har en nära koppling till de allmänna principerna för behandling av personuppgifter. Genom paragrafen genomförs artikel 27 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige innan behandlingen av personuppgifter inleds göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Skyldigheten är allmän och blir aktuell alltid när den personuppgiftsansvarige avser att inleda en i något avseende ny typ av behandling av personuppgifter eller om det sker ändringar i behandlingen av personuppgifter.

Om den bedömning som ska göras enligt 1 mom. visar att den av den personuppgiftsansvarige planerade behandlingen av personuppgifter kan medföra en betydande risk för tillgodoseendet av fysiska personers rättigheter, ska den personuppgiftsansvarige enligt *2 mom.* göra en skriftlig konsekvensbedömning. En betydande risk kan bli aktuell t.ex. när behandlingen av person-

uppgifter läggs ut, när personuppgifter överförs till tredjeländer, när det används ny databehandlingsteknik eller när informationssystem reformeras.

Konsekvensbedömningen ska innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för den registrerades rättigheter och åtgärder för att minska dem samt åtgärder för att säkerställa skyddet av personuppgifter och efterlevnaden av lagen. I synnerhet den planerade behandlingens art, omfattning, sammanhang och ändamål ska beaktas i bedömningen. Den konsekvensbedömning som avses i momentet är således mer detaljerad än den konsekvensbedömning i initialskedet som avses i 1 mom. Konsekvensbedömningarna bör omfatta t.ex. relevanta system och processer för behandling, men inte enskilda fall.

21 §. *Förhandssamråd med dataskyddsmyndigheten*. Paragrafen innehåller bestämmelser om en skyldighet att höra dataombudsmannen på förhand. Den grundar sig på artikel 28.1, 28.3, 28.4 och 28.5 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige eller personuppgiftsbiträdet i vissa situationer höra dataombudsmannen innan behandlingen av personuppgifterna inleds. Skyldigheten att höra dataombudsmannen gäller i synnerhet när den skriftliga konsekvensbedömning som avses i det föreslagna 20 § 2 mom. visar att behandlingen trots planerade skyddsåtgärder medför en betydande kvarstående risk för de registrerades rättigheter. Skyldigheten att höra dataombudsmannen på förhand aktualiseras också när behandlingen av uppgifter särskilt vid användning av ny teknik eller nya rutiner eller förfaranden medför en betydande risk för de registrerades rättigheter. Att t.ex. ta i bruk profilering som baserar sig på automatiserat beslutsfattande kan medföra en sådan betydande risk, och den personuppgiftsansvarige måste då höra dataombudsmannen på förhand. I enlighet med artikel 28.3 i direktivet kan dataombudsmannen med stöd av sina allmänna befogenheter upprätta en förteckning över sådana i momentet avsedda åtgärder i samband med vilka den personuppgiftsansvarige ska begära förhandssamråd.

Enligt *2 mom.* är den personuppgiftsansvarige skyldig att till dataombudsmannen lämna in en skriftlig konsekvensbedömning och på begäran alla andra sådana uppgifter som gör att dataombudsmannen kan bedöma lagligheten i behandlingen av personuppgifter.

Paragrafens *3 mom.* innehåller bestämmelser om de situationer då dataombudsmannen anser att den behandling som avses i 1 mom. skulle stå i strid med den föreslagna lagen. Dataombudsmannen ska då inom sex veckor från det att begäran om samråd mottogs ge den personuppgiftsansvarige och ett eventuellt personuppgiftsbiträde handledning i syfte att göra behandlingen lagenlig. Med handledning avses generellt meddelande av anvisningar och råd. Dataombudsmannen får förlänga denna period med en månad om den planerade behandlingen är så komplicerad att en förlängning krävs. I komplicerade fall kan det t.ex. uppstå behov att inhämta olika tidskrävande utredningar. Dataombudsmannen ska i sådana fall inom en månad från det att begäran om samråd mottogs informera den personuppgiftsansvarige och ett eventuellt personuppgiftsbiträde om den förlängda perioden och om skälen till fördröjningen.

4 kap. De registrerades rättigheter

22 §. *Dataskyddsbeskrivning och skyldighet att informera*. Paragrafens 1 mom. innehåller bestämmelser om en dataskyddsbeskrivning som ska göras allmänt tillgänglig. Genom paragrafen genomförs artikel 13 i dataskyddsdirektivet. Syftet med dataskyddsbeskrivningen är att informera de registrerade och andra personer om den behandling av personuppgifter som den personuppgiftsansvarige utför och på så sätt tillgodose behovet av öppenhet i uppgiftsbehandlingen. Paragrafen motsvarar delvis vad som föreskrivs om registerbeskrivning i 10 § i personuppgiftslagen. Den föreslagna dataskyddsbeskrivningen ska dock innehålla sådan information som för närvarande inte behöver tas in i en registerbeskrivning.

Enligt *1 mom.* ska den personuppgiftsansvarige tillhandahålla en aktuell skriftlig beskrivning av sådan behandling av personuppgifter som denne ansvarar för. Beskrivningen ska göras offentligt tillgänglig. Beskrivningen ska vara så aktuell som möjligt. Med skriftlig beskrivning avses också en beskrivning i elektronisk form, och beskrivningen kan finnas tillgänglig t.ex. på den personuppgiftsansvariges webbplats. Den personuppgiftsansvarige kan också efter eget val föra samma det register över behandlingar som avses i 18 § och den dataskyddsbeskrivning som avses i 22 § till en enda dataskyddsbeskrivning som är offentligt tillgänglig.

Beskrivningen ska enligt *1 punkten* för det första innehålla kontaktuppgifter för den personuppgiftsansvarige. Om den personuppgiftsansvarige har utnämnt ett dataskyddsombud, ska också dataskyddsombudets kontaktuppgifter uppges, likaså dataskyddsombudets namn, om den personuppgiftsansvarige anser det behövligt.

När det finns gemensamt personuppgiftsansvariga ska dataskyddsbeskrivningen enligt *2 punkten* innehålla också namn och kontaktuppgifter för den personuppgiftsansvariga som fungerar som kontaktpunkt för gemensamt personuppgiftsansvariga. Dessutom ska det lämnas information om att den registrerade kan utöva sina rättigheter enligt den föreslagna lagen i förhållande till var och en av de personuppgiftsansvariga. De föreslagna bestämmelserna grundar sig inte på direktivets bestämmelser om att föreskriva om saken i lag, utan det är fråga om nationell reglering.

Enligt *3 punkten* ska dataskyddsbeskrivningen innehålla uppgifter om ändamålen med och den rättsliga grunden för behandlingen, såsom den bestämmelse i lagen på vilken behandlingen av personuppgifter grundar sig.

Enligt *4 punkten* ska den period under vilken personuppgifterna kommer att bevaras framgå av beskrivningen. Om det inte är möjligt att uppge bevaringstiden t.ex. av den anledningen att bevaringstiden inte har fastställts numerärt, ska i stället kriterierna för att fastställa denna period uppges i beskrivningen, t.ex. hur ofta behovet att bevara uppgifterna ska bedömas.

Enligt *5 mom.* ska dataskyddsbeskrivningen innehålla uppgifter om eventuella sedvanliga mottagare eller kategorier av mottagare av personuppgifterna, inklusive mottagare i tredjeländer samt internationella organisationer. Alla mottagare till vilka personuppgifter eventuellt överförs eller utlämnas behöver således inte nödvändigtvis nämnas i beskrivningen. Det räcker om det i beskrivningen uppges, antingen specificerat eller kategoriserat på lämpligt sätt, till vilka mottagare personuppgifter i regel överförs eller utlämnas.

Enligt *6 punkten* ska beskrivningen också innehålla uppgifter om den registrerades rätt att av den personuppgiftsansvarige begära tillgång till personuppgifter som rör den registrerade (rätt till insyn) samt rätt att begära att personuppgifterna rättas eller utplånas eller att behandlingen av dem begränsas på det sätt som föreskrivs i 25 §. Enligt *7 punkten* ska beskrivningen också innehålla uppgifter om den registrerades rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen samt dataombudsmannens kontaktuppgifter.

I *2 mom.* föreslås bestämmelser om de situationer då den personuppgiftsansvarige ska lämna den registrerade den beskrivning som avses i 1 mom. och vissa andra uppgifter. I dessa situationer är det inte tillräckligt att den personuppgiftsansvarige gör uppgifterna allmänt tillgängliga t.ex. på sin webbplats. Den personuppgiftsansvariges informationsplikt ska i praktiken uppfyllas i situationer då den registrerades rättsskydd kräver att han eller hon informeras om de omständigheter som avses i momentet. En sådan situation kan bli aktuell t.ex. när det i speciallagstiftning föreskrivs om sådant i 13 § i denna lag avsett automatiserat individuellt beslutsfattande som har negativa rättsverkningar för den registrerade. Den registrerades rättsskydd förutsätter då att han eller hon informeras om sådana omständigheter som är av bety-

delse med tanke på utövande av den registrerades rättigheter enligt denna lag. Skyldigheten att informera den registrerade kan uppstå exempelvis också i ett sådant fall då den registrerade inte är medveten om att hans eller hennes personuppgifter har samlats in, och den registrerades rättsskydd på grund av behandlingens art eller ett procedurfel vid behandlingen förutsätter det. Den personuppgiftsansvarige ska i de fall som avses i momentet ge den registrerade den beskrivning som avses i 1 mom. och övriga sådana uppgifter som behövs för utövandet av den registrerades rättigheter, i synnerhet sådana för personen viktiga närmare uppgifter om de omständigheter som uppräknas i 1 mom.

Den personuppgiftsansvarige får låta bli att lämna den information som avses i momentet, om det är nödvändigt för att trygga en brottsutredning eller den nationella säkerheten eller på de övriga grunder som föreslås i 28 §.

De bestämmelser som föreslås i momentet grundar sig på artikel 13.2 och 13.3 i dataskyddsdirektivet.

23 §. *De registrerades rätt till insyn*. Paragrafen innehåller bestämmelser om de registrerades rätt att få tillgång till personuppgifter på det sätt som anges i artikel 14 i dataskyddsdirektivet. I den föreslagna lagen används benämningen rätt till insyn för denna rätt, på samma sätt som i 26 § i personuppgiftslagen.

Enligt paragrafen har en registrerad rätt att av den personuppgiftsansvarige få veta huruvida personuppgifter som gäller honom eller henne behandlas. Bestämmelsen förutsätter att information ges också i det fall att inga uppgifter om personen behandlas. För att få informationen ska den registrerade redogöra för de omständigheter som behövs för att söka fram uppgifterna, t.ex. på lämpligt sätt styrka sin identitet. Bestämmelser om begränsning av rätten till insyn tas in i 24 § i den föreslagna lagen.

Om personuppgifter som gäller den registrerade behandlas, ska den registrerade ha rätt att få den information som uppräknas i momentet av den personuppgiftsansvarige. Information ska enligt *1 punkten* ges om vilka personuppgifter som behandlas och all tillgänglig information om varifrån uppgifterna kommer, såsom huruvida uppgifterna kommer från den registrerade själv eller från en annan myndighet.

Enligt *2 punkten* ska den registrerade informeras om ändamålen med och den rättsliga grunden för behandlingen, såsom den bestämmelse i lagen på vilken behandlingen av personuppgifter grundar sig. Enligt *3 punkten* ska den registrerade också få information om de kategorier av personuppgifter som behandlingen gäller.

Enligt *4 punkten* ska den information som ges den registrerade innehålla eventuella mottagare eller kategorier av mottagare till vilka den registrerades personuppgifter har lämnats ut, inklusive mottagare i tredjeländer samt internationella organisationer.

Enligt *5 punkten* ska den registrerade informeras om den period under vilken personuppgifterna kommer att bevaras. Om det inte är möjligt att uppge bevaringstiden t.ex. därför att den inte har fastställts numeriskt, ska kriterierna för att fastställa perioden fastställas i andra hand i beskrivningen.

Den personuppgiftsansvarige ska också ge information om utövande av den registrerades rättigheter. Enligt *6* och *7 punkten* ska det ges information om den registrerades rätt att av den personuppgiftsansvarige yrka att de personuppgifter som rör den registrerade rättas eller utplånas eller behandlingen av dem begränsas samt rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen samt dataombudsmannens kontaktuppgifter.

I *2 mom.* föreskrivs det om förfarandet i anknytning till 1 mom. Bestämmelser om detta finns i 28 § 1 mom. i den gällande personuppgiftslagen. Enligt bestämmelsen ska den som önskar kontrollera uppgifter om sig själv på det sätt som avses i 1 mom., begära detta hos den personuppgiftsansvarige genom en egenhändigt undertecknad handling eller på ett därmed jämförbart bestyrkt sätt eller begära detta personligen hos den personuppgiftsansvarige. Bestämmelsen är teknikneutral, dvs. den gör det möjligt att tillgodose rätten till insyn t.ex. med hjälp av en elektronisk anslutning, om detta kan genomföras i enlighet med de föreslagna förutsättningarna. En begäran om att få tillgång till uppgifterna ska på samma sätt som för närvarande alltid först riktas till den personuppgiftsansvarige i fråga, om inte något annat föreskrivs i lag. I fråga om sådana register där den registrerade inte alls har rätt till insyn, kan den registrerade ta kontakt direkt med dataombudsmannen.

24 §. *Inskränkningar i rätten till insyn.* Paragrafen innehåller bestämmelser om inskränkningar i den rätt till insyn om vilken föreskrivs i 23 §. Paragrafen grundar sig på artikel 15.1, 15.3 och 15.4 i dataskyddsdirektivet. Enligt artikeln får medlemsstaterna införa lagstiftning som helt eller delvis begränsar den registrerades rätt till insyn i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Även för närvarande är det med stöd av 27 § i personuppgiftslagen möjligt att begränsa rätten till insyn. Enligt 1 mom. 1 punkten i den paragrafen har den registrerade inte rätt till insyn, om informationen kan skada statens säkerhet, försvaret eller den allmänna ordningen och säkerheten eller försvåra förebyggande eller utredning av brott. Till denna del ändras rättsläget således inte avsevärt.

Enligt *1 mom.* kan den registrerades rätt till insyn helt eller delvis skjutas upp, begränsas eller vägras till den del det är nödvändigt på de grunder som nämns i 28 §. Det kan finnas behov att skjuta upp rätten till insyn t.ex. när en part har hörts, men förundersökningen ännu inte har avslutats. Om den registrerades rätt till insyn skjuts upp, begränsas eller vägras, ska den personuppgiftsansvarige enligt momentet utan obefogat dröjsmål informera den registrerade om detta. Den registrerade ska på samma sätt som i den gällande personuppgiftslagen ges ett skriftligt intyg om saken. Även grunderna för uppskovet, begränsningen eller vägran ska enligt momentet uppges i det sammanhanget, utom i det fall att lämnandet av denna information skulle äventyra syftet med vägran eller begränsningen. Det är fortfarande möjligt att i speciallagstiftning föreskriva om begränsning av rätten till insyn i något visst register i sådana fall då en begränsning på det sätt som föreskrivs i direktivet är en nödvändig och proportionell åtgärd i ett demokratiskt samhälle, med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen.

Om den personuppgiftsansvarige inte inom tre månader efter att begäran framställts har gett den registrerade ett skriftligt svar, betraktas detta enligt momentet som att insyn har vägrats. Dataskyddsdirektivet innehåller ingen motsvarande bestämmelse, så det är fråga om nationell reglering. En motsvarande bestämmelse ingår dock i 28 § 2 mom. i den gällande personuppgiftslagen. Om den registrerade inte får uppgifterna inom tre månader, kan han eller hon vända sig till dataombudsmannen i detta ärende.

Enligt *2 mom.* ska den personuppgiftsansvarige när denne begränsar den registrerades rätt till insyn informera den registrerade om dennes rätt att lämna in en begäran om åtgärder till dataombudsmannen på grund av att rätten till insyn skjutits upp, begränsats eller vägrats samt om dennes rätt att i enlighet med 29 § utöva rätten till insyn via dataombudsmannen.

Enligt *3 mom.* är den personuppgiftsansvarige skyldig att bevara information om de grunder på vilka rätten till insyn vägrats eller begränsats. Denna information ska på begäran finnas tillgänglig för tillsynsmyndigheten. Genom att dokumentera informationen är det vid behov möjligt att i efterhand säkerställa huruvida det funnit skäl att begränsa rätten till insyn.

25 §. *Rättelse eller utplåning av personuppgifter eller begränsning av behandlingen*. Paragrafen innehåller bestämmelser om rättelse och utplåning av personuppgifter samt begränsning av behandlingen på det sätt som föreskrivs i artikel 16.1, 16.2 och 16.3 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål rätta eller komplettera sådana personuppgifter om den registrerade som är oriktiga eller bristfälliga med hänsyn till ändamålet med behandlingen. Den registrerade kan inleda sitt yrkande om rättelse eller komplettering genom att iaktta de allmänna bestämmelser i förvaltningslagen som gäller inledande av ett ärende. Den registrerade kan lämna in en ytterligare utredning utifrån vilken de bristfälliga personuppgifterna kan kompletteras. Om uppgifterna är oriktiga eller bristfälliga med hänsyn till ändamålet med behandlingen, ska de rättas eller kompletteras. Exempelvis i en situation då uppgifterna baserar sig på ett vittnes berättelse, ska uppgifterna inte betraktas som oriktiga med hänsyn till ändamålet med behandlingen, även om uppgifterna senare visar sig ha lämnats i falskt syfte. Det förfarande som avses i momentet är inte heller avsett att tillämpas t.ex. i en situation då den registrerade önskar ändra de uppgifter som antecknats i ett förhörsprotokoll, utan då ska bestämmelserna i förundersökningslagen tillämpas.

Enligt *2 mom.* är den personuppgiftsansvarige skyldig att på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål utplåna personuppgifter om den registrerade, om behandlingen av dem står i strid med bestämmelserna i 4 eller 5 §, 6 § 1 eller 2 mom. eller 7 eller 11 §. Det är då fråga om en situation då fortsatt behandling av personuppgifterna skulle innebära överträdelse av någon av nämnda bestämmelser. Det som sägs i artikel 16.2 i direktivet om att uppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige behöver inte tas in i momentet, eftersom skyldigheten att utplåna uppgifterna då grundar sig direkt på bestämmelsen i fråga.

I stället för att utplåna uppgifterna ska den personuppgiftsansvarige enligt momentet dock endast begränsa behandlingen om den registrerade bestrider uppgifternas korrekthet och det inte kan fastställas huruvida de är korrekta (*1 punkten*) eller om personuppgifterna måste bevaras som bevisning (*2 punkten*). Det kan finnas behov att bevara oriktiga personuppgifter som sedermera rättats för senare bevisning eller t.ex. för eventuell bevisning i fråga om tjänstebrott. I praktiken kan det ofta uppstå situationer då antingen den registrerades eller en myndighets berättigade rättigheter förutsätter att de oriktiga uppgifterna bevaras parallellt med de rättade.

Enligt *3 mom.* ska den personuppgiftsansvarige, om behandlingen har begränsats med stöd av 2 mom. 1 punkten, innan begränsningen upphävs informera den registrerade om detta.

26 §. *Vägran att godkänna den registrerades yrkande*. I paragrafen föreskrivs det om förfarandena vid vägran att godkänna ett yrkande som den registrerade framställt i enlighet med 25 §. Detta överensstämmer med vad som förutsätts i artikel 16.4 i dataskyddsdirektivet.

Om inte den personuppgiftsansvarige godkänner den registrerades yrkande om rättelse, komplettering eller utplåning av personuppgifter eller begränsning av behandlingen av dem, ska den personuppgiftsansvarige enligt 1 mom. informera den registrerade om vägran och grunderna för vägran. Den personuppgiftsansvarige ska ge ett skriftligt intyg om detta. Den personuppgiftsansvarige får enligt momentet helt eller delvis låta bli att lämna information om grunderna för vägran, om det är nödvändigt på de grunder som nämns i 28 §.

Enligt 2 mom. ska den personuppgiftsansvarige informera den registrerade om att denne har rätt att lämna in en begäran om åtgärder till dataombudsmannen på grund av vägran och om

att denne har rätt att i enlighet med 29 § utöva de rättigheter som avses i 25 § via dataombudsmannen.

27 §. *Den personuppgiftsansvariges skyldighet att informera om rättelse, utplåning eller begränsning av behandlingen*. Genom paragrafen genomförs artikel 16.5 och 16.6 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige anmäla varje rättelse av oriktiga personuppgifter till den myndighet från vilken de oriktiga personuppgifterna kommer. Följaktligen kan också den myndighet som ursprungligen lämnat ut uppgifterna vid behov på eget initiativ rätta de personuppgifter som den har.

Om personuppgifter har rättats eller utplånats eller behandlingen av dem har begränsats, ska den personuppgiftsansvarige enligt *2 mom.* informera de mottagare om saken till vilka den personuppgiftsansvarige har lämnat ut uppgifterna. Det utlämnande som avses i momentet inbegriper också eventuellt utlämnande till tredjeländer. Mottagarna av uppgifterna ska i sin verksamhet på lämpligt sätt beakta de åtgärder gällande personuppgifterna som den personuppgiftsansvarige meddelat samt de begränsningar som hänför sig till dem, och t.ex. rätta de oriktiga personuppgifter som mottagarna har.

28 §. *Begränsning av de registrerades rättigheter*. I paragrafen föreskrivs det om de förutsättningar under vilka det är möjligt att avvika från vissa av de rättigheter för de registrerade som anges i kapitlet. De registrerades rättigheter får begränsas på det sätt som anges i 22 § 2 mom., 24 § 1 mom., 26 § 1 mom. och 35 §, om det med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd och om någon av de situationer som uppräknas i paragrafen är aktuell. En begränsning av rättigheterna kräver således avvägning från fall till fall, och som begränsande åtgärd ska t.ex. väljas en sådan med hänsyn till syftet med begränsningen effektiv åtgärd som begränsar den registrerades rättigheter så litet som möjligt.

Enligt *1 punkten* är en begränsning av rättigheterna tillåten i en situation då begränsningen görs i syfte att undvika menlig inverkan på förebyggande, avslöjande eller utredning av brott eller på åtgärder som avser åtal för brott eller på verkställighet av straffrättsliga påföljder. Det kan t.ex. vara fråga om en situation då underlåtenhet att begränsa behandlingen av personuppgifter skulle äventyra en brottsutredning.

Enligt *2 punkten* är en begränsning tillåten om den behövs för att trygga andra undersökningar, utredningar eller motsvarande förfaranden hos myndigheter. Det kan t.ex. vara fråga om att trygga tillsynsförfarandet hos skattemyndigheterna eller någon annan myndighet. Det kan t.ex. också vara fråga om att trygga tillsynsförfarandet hos en behörig myndighet i en annan EU-stat.

Enligt *3—5 punkten* kan en begränsning bli aktuell också i syfte att skydda den allmänna säkerheten, den nationella säkerheten eller andra personers rättigheter. För att de registrerades rättigheter ska kunna begränsas måste nödvändighets- och proportionalitetsprinciperna i fråga om dessa grunder iakttas.

29 §. *Utövande av rättigheter via dataombudsmannen*. Paragrafen innehåller bestämmelser om den registrerades rätt att utöva vissa av sina rättigheter via dataombudsmannen. Genom paragrafen genomförs artikel 17.1 och 17.3 i dataskyddsdirektivet.

I *1 mom.* föreskrivs det om den rätt till insyn som den registrerade har indirekt. Enligt momentet har den registrerade rätt att be dataombudsmannen kontrollera lagenligheten i personuppgifter och behandlingen av dem, om den registrerades rätt till insyn har skjutits upp, begrän-

sats eller vägrats med stöd av denna eller någon annan lag eller om den personuppgiftsansvarige inte godkänner den registrerades yrkande om rättelse, komplettering eller utplåning av personuppgifterna eller begränsning av behandlingen av dem. Den registrerade får dock utöva dessa rättigheter först efter det att den registrerade själv har försökt utöva sina rättigheter i förhållande till den personuppgiftsansvarige, men den personuppgiftsansvarige har begränsat utövandet av den registrerades rättigheter antingen helt eller delvis. I de situationer då den registrerades rätt till insyn har begränsats direkt i lagen, blir det dock omedelbart fråga om att utöva rätten till insyn indirekt, dvs. den registrerade kan vända sig direkt till dataombudsmannen i stället för till den personuppgiftsansvarige.

När dataombudsmannen agerar för den registrerade på det sätt som avses i 1 mom. ska dataombudsmannen enligt *2 mom.* informera den registrerade om de åtgärder som ombudsmannen har vidtagit på grund av ärendet. Dataombudsmannen ska också informera den personuppgiftsansvarige om dennes rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen.

30 §. *Främjande av de registrerades möjligheter att utöva sina rättigheter samt avgiftsfria åtgärder.* Genom paragrafen genomförs artikel 12 i dataskyddsdirektivet. De krav som artikeln innehåller uppfylls delvis genom allmänna förvaltningsrättsliga bestämmelser. Bestämmelser om behandling utan dröjsmål finns t.ex. i 23 § i förvaltningslagen. Enligt den paragrafen ska ett ärende behandlas utan ogrundat dröjsmål, och en myndighet ska på en parts begäran ge en uppskattning om när ett beslut kommer att ges samt svara på förfrågningar om hur behandlingen framskrider.

Enligt *1 mom.* är den personuppgiftsansvarige skyldig att främja de registrerades möjligheter att utöva de rättigheter som avses i kapitlet. Dessa rättigheter gäller bl.a. rätten till insyn och rätten att yrka rättelse av uppgifter. Alla meddelanden och all information om behandling av personuppgifter som lämnas till de registrerade ska dessutom tillhandahållas i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma form som begäran. Också den information som finns på den personuppgiftsansvariges webbplats ska vara lättillgänglig och begriplig, vilket förutsätter ett klart och tydligt språk. Kravet på begriplig information innebär också att målgruppens mångfald ska beaktas när information lämnas.

Enligt *2 mom.* är meddelanden och information som ska ges de registrerade samt behandlingen av begäranden som de registrerade framställt i enlighet med lagen i princip avgiftsfria för de registrerade. Om en registrerads begäranden på grund av att de upprepats eller av någon annan orsak dock är uppenbart orimliga eller ogrundade, får den personuppgiftsansvarige för åtgärden ta ut en avgift enligt vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992). Den lagen innehåller bestämmelser om de allmänna grunderna för när statliga myndigheters prestationer ska vara avgiftsbelagda och för storleken av de avgifter som uppbärs för prestationerna samt om övriga grunder för avgifterna.

Enligt gällande 26 § 3 mom. i personuppgiftslagen får den registeransvarige uppbära en ersättning för lämnande av information endast om det har förflutit mindre än ett år sedan den registrerade senast fick kontrollera uppgifterna i registret. Begäranden om rätt till insyn som riktats till den personuppgiftsansvarige oftare än så är dock inte nödvändigtvis alltid orimliga. Det kan dock i princip anses orimligt t.ex. att begäranden med samma innehåll lämnas in flera gånger inom en kort tid, och då kan en avgift tas ut för åtgärderna.

Om den personuppgiftsansvarige tar ut en avgift med stöd av 2 mom. ska den personuppgiftsansvarige enligt *3 mom.* vid behov visa att begäran har varit uppenbart ogrundad eller orimlig.

Den personuppgiftsansvarige ska således i praktiken dokumentera varför det tagits ut en avgift för åtgärden.

5 kap. Informationssäkerhet

31 §. *Skydd av personuppgifter*. Paragrafen innehåller en allmän skyldighet att skydda personuppgifter. Skyldigheten gäller såväl den personuppgiftsansvarige som personuppgiftsbiträdet. Paragrafen grundar sig på artikel 4.1 f samt artikel 29.1 i dataskyddsdirektivet. Bestämmelser om skydd av uppgifterna finns för närvarande i 32 § i personuppgiftslagen.

Enligt den föreslagna paragrafen ska den personuppgiftsansvarige och personuppgiftsbiträdet genom tekniska och organisatoriska åtgärder se till att personuppgifterna är tillräckligt skyddade med hänsyn till den risk för den registrerades rättigheter som behandlingen medför. Personuppgifterna ska särskilt skyddas för obehörig behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den personuppgiftsansvarige ska på samma sätt som för närvarande t.ex. fastställa vem som får använda uppgifterna och ta i bruk lösenordssystem och andra lämpliga säkerhetsarrangemang för att säkerställa att endast personer med rätt till det kommer åt att behandla uppgifterna.

De åtgärder som avses i paragrafen ska planeras, bedömas och genomföras med beaktande av den senaste tekniska utveckling, kostnaderna för att genomföra åtgärderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter.

När kravnivån i fråga om skyddet bedöms kan man å ena sidan beakta de tekniska medel som kan användas för skyddet och de kostnader de medför. Något som å andra sidan inverkar på den informationssäkerhetsnivå som krävs är också vilka slags personuppgifter som behandlas och i vilken omfattning de behandlas. När det t.ex. gäller uppgifter som hör till särskilda kategorier av personuppgifter, bör skyddet och en informationssäker behandling ägnas särskilt mycket uppmärksamhet, och i fråga om dem är mer heltäckande skyddsåtgärder i regel befogade. Även om personuppgifterna behandlas i andra system än automatiserade behandlingssystem, ska den personuppgiftsansvarige och ett eventuellt personuppgiftsbiträde ha tillgång till effektiva metoder, såsom logguppgifter och annan slags dokumentation, genom vilken behandlingen laglighet kan visas, frivillig övervakning genomföras samt uppgifternas integritet och informationssäkerheten säkerställas.

32 §. *Skydd av personuppgifter vid automatiserad behandling*. Paragrafen innehåller bestämmelser om särskilda krav på skydd i sådana situationer då personuppgifter behandlas genom automatiserad behandling. Genom paragrafen genomförs artikel 29.2 i dataskyddsdirektivet.

Utöver vad som föreskrivs i 31 § ska den personuppgiftsansvarige eller personuppgiftsbiträdet när det gäller automatiserad behandling, efter en bedömning av riskerna, vidta lämpliga åtgärder i syfte att skydda personuppgifterna. Vid automatiserad behandling bör t.ex. en begränsning av behandlingen av personuppgifterna i princip säkerställas med tekniska medel. En begränsning av behandlingen av personuppgifter bör anges inom systemet på ett sådant sätt att det tydligt framgår att behandlingen av personuppgifterna är begränsad.

Syftet med de åtgärder som avses i paragrafen är att vägra varje obehörig person åtkomst till den utrustning som används för behandling, förhindra obehörig läsning, kopiering, ändring och utplåning av datamedier samt förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring och utplåning av lagrade personuppgifter. Dessa åtgärder ska också förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring och säkerställa att personer som är behöriga att använda ett

automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet. Behörigheten ska fastställas utifrån en behovsprövning. Behörighet ska således beviljas enbart i den omfattning som personen behöver vissa personuppgifter för att utföra sina uppgifter. Behörigheten är personlig.

Avsikten med de skyddsåtgärder som avses i paragrafen är också att säkerställa att det är möjligt att även i efterhand kontrollera och fastställa till vilka organ personuppgifter har överförts och för vilka organ de gjorts tillgängliga. Strävan är också att med deras hjälp säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes.

Enligt de föreslagna bestämmelserna ska man genom lämpliga åtgärder också försöka förhindra obehörig läsning, kopiering, ändring och utplåning av personuppgifter i samband med överföring av sådana uppgifter eller under transport av datamedier. Den personuppgiftsansvarige och personuppgiftsbiträdet ska dessutom säkerställa att de system som används kan återställas vid störningar och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet.

33 §. *Personuppgiftsbiträdets skyldighet att informera om en personuppgiftsincident*. Paragrafen innehåller bestämmelser om skyldighet för personuppgiftsbiträdet att informera om en personuppgiftsincident som han eller hon upptäckt eller fått kännedom om. Enligt paragrafen ska personuppgiftsbiträdet i en sådan situation utan obefogat dröjsmål informera den personuppgiftsansvarige om personuppgiftsincidenten. Enligt den definition som föreslås i 3 § 1 mom. 9 punkten avses med personuppgiftsincident en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Den föreslagna paragrafen grundar sig på artikel 30.2 i dataskyddsdirektivet.

34 §. *Den personuppgiftsansvariges skyldighet att anmäla en personuppgiftsincident till dataombudsmannen*. I paragrafen föreskrivs det om den personuppgiftsansvariges skyldighet att informera dataombudsmannen om en personuppgiftsincident som gäller personuppgifter. Genom paragrafen genomförs artikel 30.1, 30.2 och 30.5 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige anmäla en personuppgiftsincident till dataombudsmannen, utom när det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för den registrerades rättigheter. Genom pseudonymisering av personuppgifter och andra tekniker som gör att uppgifter inte längre kan kopplas samman med en viss registrerad är det möjligt att minska sannolikheten för att en eventuell personuppgiftsincident medför en risk för den registrerade.

Den personuppgiftsansvarige ska i enlighet med *2 mom.* göra anmälan enligt 1 mom. utan obefogat dröjsmål och om möjligt inom 72 timmar efter att ha fått kännedom om incidenten. Om anmälan görs senare än så, ska skälen till fördröjningen nämnas i anmälan.

Enligt *3 mom.* ska den personuppgiftsansvarige bevara uppgifter om personuppgiftsincidenter och omständigheter i samband med den, såsom deras effekter och de korrigerande åtgärder som vidtagits och anmälningar som gjorts.

35 §. *Den personuppgiftsansvariges skyldighet att informera den registrerade om en personuppgiftsincident*. I paragrafen föreskrivs det om en skyldighet att informera den registrerade om en personuppgiftsincident i enlighet med vad som förutsätts i artikel 31.1, 31.3 och 31.5 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige utan obefogat dröjsmål informera den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en betydande risk för den registrerades rättigheter. När en sådan risk bedöms är det skäl att beakta bl.a. slaget av personuppgifter, den kategori av registrerade som är föremål för incidenten samt omfattningen av de uppgifter som är föremål för incidenten.

Informationsskyldighet föreligger dock inte om den personuppgiftsansvarige på de personuppgifter som påverkades av personuppgiftsincidenten har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder som kan antas förhindra missbruk av uppgifterna på ett effektivt sätt. Informationsskyldighet föreligger inte heller om den personuppgiftsansvarige efter incidenten har vidtagit åtgärder för att säkerställa att incidenten sannolikt inte kommer att medföra en risk för den registrerades rättigheter. Det kan vara fråga om en sådan situation t.ex. när personuppgifter som ändrats i samband med en personuppgiftsincident har återställts i sin ursprungliga form, och det har säkerställts att de ändrade uppgifterna inte har lämnats ut eller behandlats på annat sätt under den tiden.

Enligt *2 mom.* kan den personuppgiftsansvarige i stället för att lämna information till den registrerade upplysa om personuppgiftsincidenten genom information till allmänheten, om det skulle kräva oproportionerliga ansträngningar att informera de registrerade. Att lämna personlig information till varje registrerad separat kan bli oskäligt t.ex. när personuppgiftsincidenten har riktat sig till en exceptionellt stor mängd registrerade eller när den personuppgiftsansvarige inte har de registrerades kontaktuppgifter. Sättet att lämna information till allmänheten kan väljas fritt, men informationen måste nå de registrerade på ett effektivt sätt. Kravet på allmän information kan i det enskilda fallet uppfyllas t.ex. genom ett synligt meddelande på ingångssidan på den personuppgiftsansvariges webbplats.

Enligt *3 mom.* kan informationen till den registrerade dock skjutas upp, begränsas eller i undantagsfall utelämnas, om de förutsättningar som anges i 28 § uppfylls. Eftersom det är fråga om en begränsning av de registrerades rättigheter, ska undantaget tolkas strikt.

36 §. *Den personuppgiftsansvariges skyldighet att informera andra personuppgiftsansvariga om en personuppgiftsincident*. Paragrafen innehåller bestämmelser om den personuppgiftsansvariges skyldighet att informera andra personuppgiftsansvariga om en personuppgiftsincident. Enligt paragrafen ska den personuppgiftsansvarige utan obefogat dröjsmål lämna en anmälan om en personuppgiftsincident till personuppgiftsansvariga i Finland eller i andra EU-medlemsstater, om incidenten gäller personuppgifter som har överförts av eller till de personuppgiftsansvariga i fråga. Andra personuppgiftsansvariga ska enligt den föreslagna bestämmelsen alltid informeras om en personuppgiftsincident oberoende av sannolikheten för att incidenten medför en risk för den registrerades rättigheter eller inte. På så sätt kan också en annan personuppgiftsansvarig vid behov vidta lämpliga åtgärder på grund av incidenten.

Den föreslagna paragrafen grundar sig på artikel 30.6 i dataskyddsdirektivet. Enligt artikeln ska det endast föreskrivas att en personuppgiftsansvarig i en annan medlemsstat ska informeras om incidenten. I den föreslagna paragrafen utsträcks informationsplikten dock också till inhemska personuppgiftsansvariga, när det är fråga om uppgifter som har lämnats ut till dem eller av dem.

37 §. *Innehållet i anmälan om en personuppgiftsincident*. Paragrafen innehåller bestämmelser om innehållet i en anmälan som lämnas på grund av en personuppgiftsincident. De minimikrav som ställs på en anmälan beror på till vem anmälan lämnas. Paragrafen grundar sig på artikel 30.3 och 30.4 samt 31.2 i dataskyddsdirektivet. Artikel 31.2 i direktivet genomförs dock delvis genom det föreslagna 30 § 1 mom., enligt vilket alla meddelanden och all inform-

ation om behandling av personuppgifter som lämnas till de registrerade ska tillhandahållas i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk.

Enligt *1 mom.* ska en anmälan enligt 34 § till dataombudsmannen och en anmälan enligt 36 § till andra personuppgiftsansvariga innehålla en beskrivning av personuppgiftsincidenten. Beskrivningen ska om möjligt inbegripa de kategorier av registrerade och det ungefärliga antal registrerade som berörs samt de kategorier av personuppgifter och det ungefärliga antal personuppgiftsposter som berörs.

Den information enligt 35 § som lämnas till den registrerade ska enligt *2 mom.* innehålla en beskrivning av personuppgiftsincidentens art. Av anmälan ska det således i typfallet bl.a. framgå vilka uppgifter som påverkades av personuppgiftsincidenten och huruvida det är fråga t.ex. om utplåning av uppgifter eller olaglig åtkomst till uppgifter.

I paragrafens *3 mom.* föreskrivs det också att de anmälningar och den information som avses i 1 och 2 mom. ska innehålla namnet på och kontaktuppgifter för dataskyddsombudet eller en annan kontaktpunkt där mer information kan erhållas, samt de sannolika konsekvenserna av personuppgiftsincidenten. Anmälan ska också innehålla en beskrivning av de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten och vid behov åtgärder för att mildra dess negativa effekter.

Enligt *4 mom.* får den information som lämnas till dataombudsmannen och till andra personuppgiftsansvariga tillhandahållas i omgångar till den del det inte är möjligt att tillhandahålla informationen samtidigt.

6 kap. Dataskyddsombud

38 §. *Utnämning av dataskyddsombud*. Paragrafen innehåller bestämmelser om den personuppgiftsansvariges skyldighet att utnämna ett dataskyddsombud enligt vad som förutsätts i artikel 32 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige utnämna ett dataskyddsombud för sin organisation. Dataskyddsombudet ska ha tillräcklig sakkunskap om lagstiftning och praxis i fråga om behandling av personuppgifter samt förmåga att sköta de uppgifter som avses i 40 §. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter, om det är motiverat med hänsyn till myndigheternas organisationsstruktur och storlek. När ett gemensamt dataskyddsombud utnämns bör det tas hänsyn till att dataskyddsombudet har en faktisk möjlighet att sköta sin uppgift på ett effektivt sätt för alla de behöriga myndigheternas del.

Dataskyddsombudet kan t.ex. vara en sådan anställd hos den personuppgiftsansvarige som har fått utbildning i dataskyddsrätt och praxis inom branschen för att förvärva den sakkunskap som behövs. Vad som är tillräcklig specialsakkunskap och sådan tillräcklig färdighetsnivå som avses i momentet kan anses vara beroende av i synnerhet arten av den personuppgiftsansvariges verksamhet och den behandling av personuppgifter som denne utför samt vilket skydd de uppgifter som behandlas kräver. Dataskyddsombudet kan också vara en utomstående person i förhållande till den personuppgiftsansvarige, dvs. någon som sköter uppgifterna som dataskyddsombud på basis av ett uppdragsavtal. Dataskyddsombudets uppgifter kan utföras på deltid eller heltid. Samma person kan vara dataskyddsombud enligt den föreslagna lagen och enligt allmänna dataskyddsförordningen förutsatt att de krav som uppställts i vardera författningen blir uppfyllda.

I paragrafens *2 mom.* förutsätts det att den personuppgiftsansvarige ska meddela dataombudsmannen dataskyddsombudets kontaktuppgifter och eventuella ändringar i dem.

39 §. *Dataskyddsombudets ställning*. Paragrafen innehåller bestämmelser om dataskyddsombudets ställning. Den grundar sig på artikel 33 i dataskyddsdirektivet.

Enligt *1 mom.* ska den personuppgiftsansvarige på ett korrekt sätt och i god tid se till att dataskyddsombudet deltar i alla frågor som rör skyddet av personuppgifter. Exempelvis när nya informationssystem planeras ska dataskyddsombudet på lämpligt sätt ges tillfälle att delta i planeringen av upphandlingen. Dataskyddsombudet är dock inte ansvarigt för att behandlingen av personuppgifter är laglig.

Enligt *2 mom.* ska den personuppgiftsansvarige ge dataskyddsombudet verksamhetsförutsättningar att sköta de uppgifter som denne ansvarar för enligt 40 § samt ge tillgång till personuppgifter och behandlingsförfaranden. Vid resursfördelningen ska det t.ex. tas hänsyn till att dataskyddsombudet anvisas tillräckligt med resurser för att upprätthålla sin sakkunskap.

40 §. *Dataskyddsombudets uppgifter*. Paragrafen innehåller bestämmelser om dataskyddsombudets uppgifter i enlighet med vad som föreskrivs i artikel 32.1 och artikel 34 i dataskyddsdirektivet.

Enligt *1 mom. 1 punkten* ska dataskyddsombudet för det första ge råd i frågor som gäller skydd av personuppgifter till den personuppgiftsansvarige och den personal hos den personuppgiftsansvarige som behandlar personuppgifter. Enligt *2 punkten* ska dataskyddsombudet också övervaka att de bestämmelser som gäller behandling av personuppgifter och den personuppgiftsansvariges förfaranden för behandling av personuppgifter iakttas. Till dessa uppgifter hör t.ex. att övervaka att ansvarsfördelningen i samband med behandlingen av personuppgifter iakttas, att förbättra medvetenheten i dataskyddsfrågor och att utbilda den personal som deltar i behandlingen av personuppgifter samt att utföra kontroller i anslutning till behandlingen.

Enligt *3 punkten* ska dataskyddsombudet på begäran ge råd om konsekvensbedömningen avseende dataskydd och övervaka att den genomförs i enlighet med 20 §. Dataskyddsombudet ska dessutom enligt 4 punkten samarbeta med dataombudsmannen och vara kontaktpunkt för dataombudsmannen i frågor som gäller behandling av personuppgifter. Till dessa frågor hör bl.a. sådant förhandssamråd med dataombudsmannen som avses i 21 § och vid behov samråd med dataombudsmannen i andra möjliga frågor.

Enligt *2 mom.* ska dataskyddsombudets uppgifter inte omfatta rättskipningsverksamhet i domstolarna eller laglighetskontroll som utförs av justitiekanslern i statsrådet och riksdagens justitieombudsman. Förslaget grundar sig på artikel 32.1 i dataskyddsdirektivet.

7 kap. Överföringar av personuppgifter till tredjeländer och internationella organisationer

41 §. *Allmänna principer för överföring av personuppgifter*. Paragrafen innehåller bestämmelser om allmänna principer för överföring av personuppgifter till tredjeländer och internationella organisationer. Bestämmelsen grundar sig på artikel 35 och 36.1 i dataskyddsdirektivet.

Som överföring av personuppgifter betraktas på samma sätt som för närvarande alla situationer då den personuppgiftsansvarige gör personuppgifter tillgängliga för en aktör i ett tredjeland eller en internationell organisation. Som överföring betraktas således t.ex. överföring av personuppgifter per e-post eller annars på elektronisk väg, såsom rätt att se uppgifter genom elektronisk anslutning samt lagring av personuppgifter i en molntjänst. Som egentligt utlämnande betraktas däremot situationer då den personuppgiftsansvarige lämnar ut personuppgifter

till en annan personuppgiftsansvarig, som kan behandla dem för sina egna ändamål. Såsom för närvarande betraktas också utlämnande som överföring av personuppgifter.

De bestämmelser som avser överföring av personuppgifter till utlandet gäller all faktisk överföring av personuppgifter till utlandet. Bestämmelserna ska således omfatta såväl egentligt utlämnande av personuppgifter som överföring av dem till tredjeländer t.ex. som en följd av att databehandlingen lagts ut. Mängden uppgifter eller hur länge överföringen pågår inverkar inte på de föreslagna bestämmelsernas tillämplighet. Endast en behörig myndighet som är personuppgiftsansvarig får överföra personuppgifter, men den personuppgiftsansvarige kan ge ett personuppgiftsbiträde i uppgift att överföra uppgifterna på sina vägnar.

Enligt *1 mom.* får en behörig myndighet överföra personuppgifter till ett tredjeland eller en internationell organisation endast om de övriga bestämmelser som är tillämpliga på behandling av personuppgifter enligt den föreslagna lagen iakttas och alla de förutsättningar som uppräknas i momentet är uppfyllda. Till de överföringar som avses i momentet räknas vidareöverföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation.

I *1 punkten* förutsätts att överföringen för det första behövs för ett ändamål som nämns i 1 § 1 mom. i den föreslagna lagen. Personuppgifter får således överföras till ett tredjeland eller en internationell organisation endast om överföringen behövs för de ändamål som uppräknas i momentet i fråga, såsom för förebyggande, utredning och avslöjande av brott eller åklagarverksamhet som har samband med brott.

För att överföringen ska vara laglig ska personuppgifterna enligt *2 punkten* överföras till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är behörig att behandla personuppgifterna för ett ändamål som nämns i 1 § 1 mom. I *3 punkten* förutsätts det dessutom att det finns ett i artikel 36 i dataskyddsdirektivet avsett giltigt beslut av Europeiska kommissionen om adekvat dataskyddsnivå i det land till vilket personuppgifterna är tänkta att överföras. Om inget sådant giltigt beslut av kommissionen finns, ska lämpliga skyddsåtgärder föreligga i enlighet med den föreslagna 42 §. Om inte heller några lämpliga skyddsåtgärder har vidtagits, får personuppgifterna överföras endast om undantag för särskilda situationer blir tillämpliga i enlighet med 43 §.

Om personuppgifterna har erhållits från en annan EU-medlemsstat, är en ytterligare förutsättning för överföring enligt *2 mom.* att medlemsstaten i fråga har gett tillstånd till överföringen på förhand. Överföringar som görs utan ett sådant tillstånd är dock tillåtna i undantagsfall, om överföringen är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en stat eller mot en EU-medlemsstats väsentliga intressen och tillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska dock informeras om överföringen utan dröjsmål.

I *3 mom.* föreskrivs att om personuppgifterna överförs vidare till ett annat tredjeland eller en annan internationell organisation, får den behöriga myndighet som gjorde den ursprungliga överföringen godkänna vidareöverföringen med iakttagande av bestämmelserna i 1 och 2 mom. och med vederbörligt beaktande av brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i det tredjeland till vilket eller den internationella organisation till vilken personuppgifterna förs vidare, samt andra relevanta omständigheter.

42 §. *Överföring på basis av lämpliga skyddsåtgärder*. Genom paragrafen genomförs artikel 37 i dataskyddsdirektivet. Om kommissionen inte har antagit ett beslut som avses i 41 § 1 mom. 3 punkten, får personuppgifter enligt *1 mom.* dock i vissa situationer överföras till ett tredjeland eller en internationell organisation, om de övriga förutsättningar som anges i 41 §

uppfylls. En ytterligare förutsättning utöver de övriga förutsättningarna är att lämpliga skyddsåtgärder för personuppgifter har fastställts i en rättsligt bindande handling eller alternativt att den personuppgiftsansvarige efter att ha bedömt alla omständigheter kring en överföring av personuppgifter drar slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

Sådana rättsligt bindande handlingar som avses i den föreslagna *1 mom. 1 punkten* kan t.ex. vara rättsligt bindande bilaterala överenskommelser som genomförts genom en nationell lag. I en sådan handling ska det säkerställas att kraven på skydd för personuppgifter iakttas och att de registrerades rättigheter respekteras och att effektiva rättsmedel existerar. I fråga om de lämpliga skyddsåtgärder som avses i *2 punkten* kan den personuppgiftsansvarige bl.a. ta hänsyn till att personuppgiftsöverföringarna kommer att omfattas av tystnadsplikt och principen om ett specifikt ändamål med behandlingen, vilket säkerställer att uppgifter inte behandlas för andra ändamål än de uttryckliga ändamålen med respektive överföring. Den personuppgiftsansvarige ska dessutom ta hänsyn till för vilket syfte personuppgifterna kommer att användas och i synnerhet att uppgifterna inte används t.ex. för att meddela dödsstraff eller för någon form av omänsklig behandling.

Enligt *2 mom*. ska den personuppgiftsansvarige informera dataombudsmannen om de kategorier av överföringar som gjorts enligt 1 mom. 2 punkten. Uppgifterna om överföringarna i fråga ska bevaras så att de på begäran kan göras tillgängliga för dataombudsmannen. Uppgifterna ska innehålla information åtminstone om datum och tidpunkt för överföringarna, den mottagande behöriga myndigheten, grunderna för överföringarna och de personuppgifter som har överförts.

43 §. *Undantag i särskilda situationer*. Paragrafen innehåller bestämmelser om de grunder för undantag med stöd av vilka personuppgifter kan överföras till ett tredjeland eller en internationell organisation i de fall då kommissionen inte har antagit ett i 41 § 1 mom. 3 punkten avsett beslut och sådana lämpliga skyddsåtgärder för uppgiftsöverföringen som förutsätts i 42 § inte föreligger. För att en överföring ska kunna göras måste de allmänna förutsättningar för överföring av uppgifter som föreslås i 41 § vara uppfyllda. Eftersom det i de förutsättningar som tas in i paragrafen är fråga om undantag från förutsättningarna för överföring av uppgifter, ska förutsättningarna tolkas på ett inskränkande sätt. Paragrafen grundar sig på artikel 38 i dataskyddsdirektivet.

Enligt *1 mom. 1—3 punkten* är en överföring möjlig endast om den är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person, för att skydda intressen som är berättigade och av stor betydelse för den registrerade eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en EU-medlemsstat eller ett tredjeland. Det kan vara fråga om att skydda intressen av grundläggande betydelse t.ex. när en uppgiftsöverföring behövs för att skydda den registrerades eller någon annan persons liv. En förutsättning för överföring av personuppgifter i syfte att skydda den registrerades berättigade intressen är att den registrerades intresse väger tungt. Det är till denna del fråga om en i direktivet tillåten extra förutsättning för överföring av personuppgifter.

Enligt *4 punkten* är en överföring möjlig i enskilda fall för de ändamål som nämns i 1 § 1 mom. eller för att fastställa, göra gällande eller försvara rättsliga anspråk som hänför sig till dem. Enligt sin ordalydelse kan den grund för överföring som avses i 4 punkten bli aktuell endast i enskilda fall, och bestämmelsen kan inte användas som rättsgrund t.ex. vid sedvanlig uppgiftsöverföring.

I *2 mom.* föreskrivs det dock om en skyldighet att göra en intresseavvägning mellan olika rättigheter innan personuppgifter överförs på basis av 1 mom. 4 punkten. Personuppgifter får inte

överföras med stöd av 4 punkten, om den berörda registrerades rättigheter ska anses väga tyngre än det allmännas intresse av en sådan överföring. Om det t.ex. är sannolikt att den registrerade utsätts för hot om våld eller blir föremål för förföljelse på grund av uppgiftsöverföringen, är det i allmänhet befogat att låta bli att överföra uppgifterna.

Uppgifter om överföringar som baserar sig på det föreslagna 1 mom. ska enligt 3 mom. bevaras och på begäran göras tillgängliga för dataombudsmannen. Sådana uppgifter ska innehålla information åtminstone om datum och tidpunkt för överföringen, den mottagande behöriga myndigheten, grunderna för överföringen och de personuppgifter som har överförts.

44 §. *Överföring av personuppgifter till enskilda mottagare och andra mottagare i tredjeländer*. Paragrafen innehåller bestämmelser om överföring av personuppgifter till enskilda mottagare och andra mottagare i tredjeländer. Sådana mottagare är enligt definitionen i regel andra än myndigheter som kan jämställas med behöriga myndigheter. Paragrafen grundar sig på artikel 39 i dataskyddsdirektivet. I artikeln ges det möjlighet att föreskriva om saken, men förpliktigar ändå inte till det.

I *1 mom.* föreskrivs det om de förutsättningar under vilka en behörig myndighet trots vad som föreskrivs i 41 § 1 mom. 2 punkten i ett enskilt fall får överföra personuppgifter direkt till enskilda och andra mottagare som är etablerade i tredjeländer. Samtliga i momentet uppräknade förutsättningar ska uppfyllas samtidigt. De överföringar som avses i paragrafen blir aktuella endast i undantag och i enskilda fall.

En överföring är tillåten i synnerhet när den i enlighet med *1 punkten* är nödvändig för att en överförande behörig myndighet ska kunna utföra en uppgift enligt 1 § 1 mom. som den har ansvar för. På grund av kravet på nödvändighet får uppgifter inte överföras om nämnda uppgifter kan skötas på något annat sätt som ingriper mindre i den registrerades rättigheter. Enligt *2 punkten* är en förutsättning för överföring också att den behöriga myndighet som överför uppgifterna, i sina slutsatser efter att ha bedömt frågan, anser att de berörda registrerades rättigheter inte väger tyngre än det allmänna intresse som gör överföringen behövlig i det aktuella fallet. Den överförande myndigheten ska alltså göra en noggrann intresseavvägning till denna del.

En förutsättning för överföring är enligt *3 punkten* också att den behöriga myndighet som överför uppgifterna, på grund av ärendets brådskande natur eller av någon annan orsak, anser att en överföring till en behörig myndighet i tredjelandet skulle vara ineffektiv eller olämplig. I *§* förutsätts emellertid att en sådan behörig myndighet i tredjelandet har informerats om överföringen utan obefogat dröjsmål, om inte detta skulle vara ineffektivt eller olämpligt.

Enligt *5 punkten* ska den behöriga myndighet som överför uppgifterna informera mottagaren om det eller de specifika ändamål för vilket eller vilka denne får behandla personuppgifterna och att uppgifterna får behandlas endast under förutsättning att en sådan behandling är nödvändig. Mottagaren ska också informeras om att uppgifterna inte får behandlas för andra ändamål.

Enligt *6 punkten* får överföringen inte strida mot Finlands internationella avtalsförpliktelser.

Dessutom ska de övriga bestämmelserna i den föreslagna lagen iakttas vid överföringen.

Enligt *2 mom.* är den behöriga myndigheten skyldig att bevara information om varje överföring som utförts med stöd av 1 mom. och att informera dataombudsmannen om överföringen. Den information som avses i momentet ska lämnas utan obefogat dröjsmål.

8 kap. Tillsynsmyndighet

45 §. *Dataombudsmannen*. Paragrafen innehåller bestämmelser om nationell tillsynsmyndighet på lagens tillämpningsområde. Nationell tillsynsmyndighet är i Finland samma organ som på allmänna dataskyddsförordningens och den föreslagna dataskyddslagens område, dvs. dataombudsmannen.

Genom paragrafen genomförs till behövliga delar artikel 41, 42 och 45 i dataskyddsdirektivet. Största delen av de bestämmelser som gäller organisationen vid dataombudsmannens byrå tas in i den föreslagna dataskyddslagen. Det föreslås inte att exempelvis artikel 42.5 genomförs genom denna lag, eftersom det i den föreslagna dataskyddslagen tas in bestämmelser om dataombudsmannens personal och om att dataombudsmannen utnämner personalen vid dataombudsmannens byrå.

Tillsyn över efterlevnaden av den föreslagna lagen ska enligt *1 mom.* utövas av dataombudsmannen enligt 8 § i dataskyddslagen.

Enligt *2 mom.* ska bestämmelserna om tillsyn i den föreslagna lagen inte tillämpas på domstolarna, justitiekanslern i statsrådet och riksdagens justitieombudsman. Bestämmelserna grundar sig på artikel 45.2 i dataskyddsdirektivet. Strävan med bestämmelserna är framför allt att trygga domstolarnas och de högsta laglighetsövervakarnas oberoende när det sköter uppgifter som omfattas av den föreslagna lagens tillämpningsområde. I enlighet med vad som föreskrivs i 108 och 109 § i grundlagen övervakar justitiekanslern och justitieombudsmannen lagligheten i domstolarnas verksamhet. De övervakar också att domstolarna i all sin verksamhet iakttar lagstiftningen om skydd för personuppgifter.

Enligt *3 mom.* är dataombudsmannen självständig och oberoende vid skötseln av sina uppgifter enligt den föreslagna lagen. Detta innebär bl.a. att det inte bör vara möjligt att direkt eller indirekt utifrån påverka anställda hos tillsynsmyndigheten när de sköter sina uppgifter och utövar sina befogenheter. De bör inte heller till denna del ta emot instruktioner från någon utomstående aktör.

46 §. *Uppgifter*. I paragrafen föreskrivs det om dataombudsmannens uppgifter på den föreslagna lagens tillämpningsområde. Paragrafen grundar sig på artikel 46 i dataskyddsdirektivet. De uppgifter som dataombudsmannens har enligt den föreslagna lagen skiljer sig till vissa delar från de uppgifter som dataombudsmannen påförts i artikel 59 i allmänna dataskyddsförordningen.

I *1 mom.* uppräknas dataombudsmannens uppgifter. Enligt *1 punkten* omfattar uppgifterna, utöver att utöva tillsyn över efterlevnaden av den föreslagna lagen, att öka allmänhetens medvetenhet om risker, lagstiftning, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter. Enligt *2 punkten* ska dataombudsmannen också öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om deras skyldigheter enligt den föreslagna lagen. Ett sätt att fullgöra dessa uppgifter är t.ex. att publicera instruktioner och utbilda personuppgiftsansvariga.

Till dataombudsmannens uppgifter hör enligt *3* och *4 punkten* att på begäran tillhandahålla information till registrerade om hur de ska utöva de rättigheter de har enligt den föreslagna lagen samt att ge rådgivning vid förhandssamråd enligt 21 §. Dataombudsmannen ska enligt *5 punkten* göra utredningar om efterlevnaden av den föreslagna lagen. Ombudsmannen beslutar självständigt om att göra de utredningar som ombudsmannen anser behövliga. En utredning kan t.ex. gälla något visst förvaltningsområde eller något visst sätt att behandla uppgifter. Da-

taombudsmannens uppgift är enligt *6 punkten* också att kontrollera lagligheten i behandlingen i enlighet med 29 §.

Enligt *7 punkten* ska dataombudsmannen behandla begäranden om åtgärder från registrerade eller från samfund som avses i 56 §. Dataombudsmannen ska i enlighet med vad som föreskrivs i förvaltningslagen inom skälig tid informera den som lämnat in begäran om åtgärder hur utredningen fortskrider och om resultatet. Dataombudsmannen ska i enlighet med artikel 46.2 i dataskyddsdirektivet underlätta inlämningen av sådana begäranden om åtgärder som avses i denna punkt genom åtgärder, såsom att tillhandahålla en allmänt tillgänglig blankett för begäran om åtgärder, t.ex. på sin webbplats.

Enligt *8 punkten* ska dataombudsmannen följa sådan teknisk och annan utveckling som påverkar skyddet av personuppgifter.

Enligt *2 mom.* ska dataombudsmannen bidra till verksamheten i den dataskyddsstyrelse som inrättats genom allmänna dataskyddsförordningen. I artikel 51 i dataskyddsdirektivet uppräknas dataskyddsstyrelsens uppgifter på direktivets tillämpningsområde. Styrelsens uppgift är bl.a. att utfärda rekommendationer och föra fram bästa praxis när det gäller tillämpningen av direktivet. Dataombudsmannen får således inte föra ett ärende till dataskyddsstyrelsen då det är fråga om sådan behandling av personuppgifter som faller utanför direktivets tillämpningsområde, dvs. behandling som sker i samband med verksamhet som avses i 1 § 2 mom.

Enligt *3 mom.* är dataombudsmannens åtgärder avgiftsfria för registrerade och för dataskyddsombud. Om en registrerads eller ett dataskyddsombuds begäranden dock på grund av att de upprepas eller av någon annan orsak är uppbenbart orimliga eller ogrundade, kan dataombudsmannen ta ut en avgift för åtgärderna på det sätt som föreskrivs i lagen om grunderna för avgifter till staten eller lämna det ärende som begäran gäller utan prövning. Endast i mycket exceptionella situationer kan det bli aktuellt att lämna ärendet utan prövning. En sådan situation kan uppstå t.ex. om ärendet redan har inletts vid dataombudsmannens byrå.

Om dataombudsmannen på det sätt som avses i 3 mom. tar ut en avgift eller lämnar ärendet utan prövning, ska dataombudsmannen enligt *4 mom.* vid behov kunna visa att begäran är uppenbart ogrundad eller orimlig.

47 §. *Rätt att få information*. Paragrafen innehåller bestämmelser om dataombudsmannens rätt att få information. Genom paragrafen genomförs artikel 26 och artikel 47.1 i dataskyddsdirektivet. I dataskyddsdirektivet förutsätts det att varje tillsynsmyndighet har effektiva undersökningsbefogenheter. Dessa befogenheter ska åtminstone inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna utföra sina uppgifter.

Enligt *1 mom.* har dataombudsmannen trots sekretessbestämmelserna rätt att avgiftsfritt få en i 22 § avsedd beskrivning över behandlingsåtgärderna, de i 19 § avsedda logguppgifterna samt övriga uppgifter som behövs för att dataombudsmannen ska kunna sköta sina uppgifter.

En i huvuddrag liknande bestämmelse ingår i 39 § 1 mom. i personuppgiftslagen, enligt vilket dataombudsmannen utan hinder av sekretessbestämmelserna har 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.

I *2 mom.* föreskrivs det om dataombudsmannen rätt att av personuppgiftsansvariga och personuppgiftsbiträden få upplysningar om omständigheter som dataombudsmannen behöver för att kunna sköta sina uppgifter. Upplysningar kan begäras t.ex. om sådana omständigheter som

behövs för skötseln av dataombudsmannens uppgifter och som klarlägger den information som dataombudsmannen får med stöd av sin rätt till information eller som dataombudsmannen annars behöver få för att kunna sköta sina uppgifter. Den personuppgiftsansvarige och personuppgiftsbiträdet är dessutom även annars på begäran skyldiga att samarbeta med dataombudsmannen för att denne ska kunna utföra sina uppgifter.

48 §. *Rätt att utföra inspektioner*. Paragrafen innehåller bestämmelser om dataombudsmannens rätt att utföra inspektioner i enlighet med vad som förutsätts i artikel 47.1 och 47.4 i dataskyddsdirektivet. Syftet med bestämmelserna är att se till att dataombudsmannen har effektiva inspektionsbefogenheter samt att de rättsskyddsgarantier som hänför sig till dem förverkligas.

Enligt *1 mom.* får dataombudsmannen utföra inspektioner i en personuppgiftsansvarigs eller ett personuppgiftsbiträde utrymmen, om en inspektion behövs för tillsynen över efterlevnaden av den föreslagna lagen.

I *2 mom.* ingår en ytterligare förutsättning för att utföra inspektioner när inspektionen utförs i utrymmen som används för boende av permanent natur. Inspektion får då utföras endast om det är nödvändigt för att utreda de omständigheter som är föremål för inspektion och det i det aktuella fallet finns motiverade och specificerade skäl att misstänka att det har skett eller kommer att ske en sådan överträdelse av bestämmelserna om behandling av personuppgifter att påföljden kan vara ett straff enligt strafflagen.

I 3 mom. föreslås det för klarhetens skull en bestämmelse om att 39 § i förvaltningslagen ska iakttas i samband med inspektioner. I 39 § i förvaltningslagen ingår bestämmelser om vissa krav på förfarandet vid förrättande av inspektion.

49 §. *Handräckning*. I paragrafen föreskrivs det om dataombudsmannens rätt att få handräckning av polisen för att utföra sina uppgifter. Handräckning ges på begäran av dataombudsmannen. Motsvarande bestämmelser finns även för närvarande i 8 § i lagen om datasekretessnämnden och dataombudsmannen. Handräckning kan bli aktuellt t.ex. i samband med en inspektion som avses i 48 §, om dataombudsmannen hindras att utföra sina tjänsteuppdrag eller om polisbefogenheter annars behöver användas i dataombudsmannens uppgifter.

50 §. *Anlitande av sakkunniga*. Paragrafen innehåller bestämmelser om dataombudsmannens rätt att anlita utomstående sakkunniga. Skyddet av personuppgifter berör många olika delområden i samhället. Den specialkunskap som skötseln av dataombudsmannens uppgifter förutsätter kan i vissa fall förutsätta biträde av utomstående sakkunniga. Utomstående sakkunniga kan anlitas t.ex. i en situation då det behövs särskilda insikter i krypteringsteknik eller andra utvecklade informationssäkerhetsmetoder. Dataskyddsdirektivet förutsätter inte uttryckligen att det föreskrivs om saken i medlemsstaternas lagstiftning, men de föreslagna bestämmelserna bidrar till en effektiv skötsel av dataombudsmannens uppgifter.

Enligt *1 mom.* får dataombudsmannens höra utomstående sakkunniga och begära utlåtanden från dem. Även i 7 § i lagen om datasekretessnämnden och dataombudsmannen föreskrivs det om dataombudsmannens och datasekretessnämndens rätt att höra sakkunniga och begära in utlåtanden av dem.

Enligt *2 mom.* får dataombudsmannen vid inspektioner som avses i 48 § anlita biträde av utomstående sakkunniga. Enligt momentet kan dataombudsmannen till sakkunnig utse en person som givit sitt samtycke till uppdraget och som innehar avsevärd sakkunskap med tanke på skötseln av ombudsmannens uppgifter. En sakkunnig kan inte utföra en inspektion självständigt, utan den sakkunniges uppgift är av assisterande karaktär.

Enligt *3 mom.* tillämpas på en sakkunnig bestämmelserna om tjänsteansvar när den sakkunnige utför uppgifter som avses i paragrafen. I momentet finns dessutom en hänvisning till skadeståndsansvar enligt skadeståndslagen.

51 §. *Åtgärder*. Paragrafen innehåller bestämmelser om dataombudsmannens befogenheter. Paragrafen grundar sig på artikel 47 i dataskyddsdirektivet. I paragrafen föreslås det mer omfattande befogenheter för dataombudsmannen än vad som förutsätts i dataskyddsdirektivet. När befogenheterna fastställts har strävan varit att de i tillämpliga delar och så långt det är möjligt ska överensstämma med befogenheterna i allmänna dataskyddsförordningen och att en effektiv tillsyn över skyddet av personuppgifter ska genomföras också på den föreslagna lagens område.

Enligt paragrafen kan dataombudsmannen i ärenden som omfattas av tillämpningsområdet för den föreslagna lagen ge den personuppgiftsansvarige handledning vid det förfarande för förhandssamråd som avses i 21 § (*1 punkten*), informera den personuppgiftsansvarige eller personuppgiftsbiträdet om påstådda överträdelser av bestämmelserna i den föreslagna lagen (*2 punkten*) och utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar kan stå i strid med den föreslagna lagen (*3 punkten*). Enligt *4 punkten* kan dataombudsmannen ge den personuppgiftsansvarige eller personuppgiftsbiträdet en anmärkning, om denne behandlat personuppgifter i strid med lag. En anmärkning innebär i praktiken att dataombudsmannen delger tillsynsobjektet sin motiverade ståndpunkt för framtiden om hur de bestämmelser som gäller behandling av personuppgifter borde tillämpas i vissa situationer. En anmärkning blir aktuell i en situation då det inte finns behov att vidta strängare åtgärder.

De åtgärder som uppräknas i 1—4 punkten är till karaktären något lättare än åtgärderna i 5—10 punkten. Med stöd av de sistnämnda bestämmelserna kan dataombudsmannen bl.a. ålägga den personuppgiftsansvarige eller personuppgiftsbiträdet att iaktta den registrerades begäranden om att utöva den registrerades rättigheter enligt den föreslagna lagen eller meddela ett tillfälligt eller bestående förbud eller ställa upp någon annan tillfällig eller bestående begränsning av behandlingen. Dessutom kan dataombudsmannen ålägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med bestämmelserna i den föreslagna lagen, vid behov på ett bestämt sätt och inom en rimlig tid.

Enligt artikel 47.5 i dataskyddsdirektivet ska varje medlemsstat i lag säkerställa att varje nationell tillsynsmyndighet har befogenhet att göra rättsliga myndigheter uppmärksamma på överträdelser av de bestämmelser som antas i enlighet med direktivet och att, när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden, i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med direktivet. Även om det inte tas in någon uttrycklig bestämmelse om saken i den föreslagna lagen, ska dataombudsmannen ha rätt att göra en polisanmälan om dataombudsmannen misstänker att det på ett straffbart sätt har brutits mot bestämmelserna i den föreslagna lagen.

52 §. *Vite*. Enligt *1 mom.* får dataombudsmannen förena ett i 51 § 5—10 punkten avsett beslut samt ett sådant föreläggande att lämna ut uppgifter som grundar sig på 47 § med vite. Bestämmelser om föreläggande och utdömande av vite finns i viteslagen (1113/1990).

I *2 mom.* föreslås bestämmelser om s.k. skydd mot självinkriminering för en fysisk person i samband med skyldigheten att lämna ut uppgifter. Vite kan inte riktas mot personen om det finns anledning att misstänka personen för brott och uppgifterna gäller en omständighet som har samband med brottsmisstanken.

53 §. *Hörande av dataombudsmannen*. Paragrafen innehåller bestämmelser om i vilka situationer andra myndigheter ska höra dataombudsmannen. Förslaget grundar sig framför allt på de bestämmelser om att föreskriva om saken i lag som ingår i artikel 28.2 och 47.3 i dataskyddsdirektivet. Enligt dessa artiklar ska medlemsstaterna föreskriva att tillsynsmyndigheten ska rådfrågas under utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling och att tillsynsmyndigheten på eget initiativ eller på begäran kan avge yttranden i frågor som rör skydd av personuppgifter.

I *1 mom.* föreskrivs det i enlighet med dataskyddsdirektivet att dataombudsmannen på eget initiativ eller på begäran kan yttra sig i frågor som hänför sig till sådan behandling av personuppgifter som avses i 1 §.

Enligt *2 mom.* ska dataombudsmannen ges tillfälle att bli hörd vid beredningen av lagstiftnings- eller förvaltningsreformer som gäller sådan behandling av personuppgifter som avses i 1 §. Syftet med den föreslagna bestämmelsen är att ge dataombudsmannen tillfälle att redan vid beredningen påverka lagstiftnings- och förvaltningsreformer som gäller behandlingen av personuppgifter. En bestämmelse med motsvarande innehåll ingår i 41 § 1 mom. i personuppgiftslagen.

I strafflagen föreskrivs det om hörande av dataombudsmannen när åklagaren eller en domstol behandlar ett brottmål. Åklagaren ska enligt 38 kap. 10 § i strafflagen (39/1889) höra dataombudsmannen innan åtal väcks för sekretessbrott, sekretessförseelse, kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet eller dataintrång, om brottet i fråga riktar sig mot ett personregister, samt innan åtal väcks för personregisterbrott. När domstolen behandlar ett mål som gäller ett sådant brott ska den ge dataombudsmannen tillfälle att bli hörd. I regeringens proposition med förslag till dataskyddslag föreslås det vissa ändringar i paragrafen i fråga.

54 §. *Ömsesidigt bistånd*. Paragrafen innehåller bestämmelser om ömsesidigt bistånd mellan tillsynsmyndigheterna. Genom paragrafen genomförs artikel 50.1, 50.2 och 50.7 i dataskyddsdirektivet.

Enligt *1 mom.* ska dataombudsmannen avgiftsfritt ge motsvarande tillsynsmyndighet i en annan EU-medlemsstat de personuppgifter som myndigheten nödvändigt behöver i sitt tillsynsuppdrag samt andra behövliga uppgifter, och vid behov även annars bistå myndigheten vid utövandet av tillsynen. Uppgifterna ska också innefatta sekretessbelagda uppgifter. Dessutom ska dataombudsmannen vidta också andra behövliga åtgärder för att säkerställa ett effektivt samarbete. Trots att det ömsesidiga biståndet i princip är avgiftsfritt, kan tillsynsmyndigheter komma överens med andra tillsynsmyndigheter om regler för ersättning för särskilda utgifter i samband med tillhandahållande av ömsesidigt bistånd under exceptionella förhållanden.

Det ömsesidiga biståndet ska särskilt omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om att genomföra samråd, inspektioner och utredningar. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med och skälen till denna. Information som utbytts får användas endast för det syfte för vilket den har begärts. De uppgifter som andra tillsynsmyndigheter begärt ska dataombudsmannen som regel sända på elektronisk väg med användning av ett standardiserat format, såsom det förutsätts i artikel 50.6 i dataskyddsdirektivet.

Enligt *2 mom.* ska dataombudsmannen besvara en begäran från en tillsynsmyndighet som avses i 1 mom. utan obefogat dröjsmål och inte senare än en månad efter det att dataombuds-

mannen tagit emot begäran. Sådana åtgärder kan särskilt omfatta översändande av relevant information om genomförandet av en pågående utredning.

9 kap. Rättsskydd

55 §. *Rapportering av överträdelser*. Genom paragrafen genomförs artikel 48 i dataskyddsdirektivet, enligt vilken medlemsstaterna ska föreskriva att de behöriga myndigheterna ska inrätta effektiva mekanismer för att uppmuntra till konfidentiell rapportering av överträdelser av detta direktiv. Någon motsvarande bestämmelse ingår inte i den nuvarande nationella lagstiftningen om skydd för personuppgifter. Motsvarande rapporteringskanaler genom vilka rapporter om lagöverträdelser kan lämnas (eng. whistleblowing) är dock obligatoriska t.ex. för kreditinstitut med stöd av 7 kap. 6 § i kreditinstitutslagen (610/2014) samt för försäkringsbolag med stöd av 6 kap. 17 a § i försäkringsbolagslagen (521/2008).

Enligt *1 mom.* ska den behöriga myndigheten ha förfaranden som gör det möjligt att konfidentiellt till myndigheten rapportera en misstänkt överträdelse av bestämmelserna i den föreslagna lagen. Rapporteringsförfarandet ska omfatta lämpliga och tillräckliga åtgärder för att ordna en korrekt behandling av rapporterna. Rapporteringsförfarandet ska dessutom omfatta anvisningar som tryggar skyddet för rapportörens identitet. För att systemet ska fungera måste det finnas klara instruktioner för tillvägagångssätten. Dessutom måste systemet vara lätt att använda.

Enligt *2 mom.* ska den behöriga myndigheten bevara behövlig information som sådana rapporter som avses i 1 mom. Informationen ska avföras fem år efter rapporteringen, om inte informationen fortsättningsvis behövs för en brottsutredning, en pågående rättegång eller en myndighetsundersökning eller för att trygga de rättigheter som rapportören eller den som är föremål för rapporten har. Behovet av fortsatt bevarande av uppgifterna ska i vilket fall som helst undersökas senast tre år efter den föregående kontrollen. En anteckning ska göras om kontrollen. Information som visat sig vara oriktig eller onödig ska dock avföras ur registret utan dröjsmål.

I *3 mom.* föreskrivs det om en begränsning i den registrerades rätt att få veta rapportörens identitet. Om en fysisk person till den behöriga myndigheten har lämnat en rapport som avses i 1 mom. om en misstänkt överträdelse av bestämmelserna i den föreslagna lagen, ska rapportörens identitet hållas hemlig, om det utifrån omständigheterna kan bedömas vara till nackdel för rapportören att hans eller hennes identitet röjs, i form av exempelvis motåtgärder eller diskriminering.

56 §. *Rätt att föra ärenden till dataombudsmannen*. Paragrafen innehåller bestämmelser om en registrerads rätt att föra ärenden till dataombudsmannen. Genom paragrafen genomförs i synnerhet artikel 52.1 samt artikel 55 i dataskyddsdirektivet. Möjligheten att föra ett ärende till den nationella tillsynsmyndigheten för behandling är ett betydande rättsmedel, om vilket det enligt dataskyddsdirektivet ska föreskrivas i medlemsstaternas lagstiftning.

Enligt första meningen i *1 mom.* har en registrerad rätt att föra ett ärende till dataombudsmannen för behandling, om den registrerade anser att någon vid behandlingen av hans eller hennes personuppgifter bryter mot den föreslagna lagen eller någon annan lag som gäller behandling av personuppgifter. Om denna rättighet för den registrerade används i lagen också uttrycket ”begäran om åtgärder”. Med stöd av bestämmelserna i momentet ska den registrerade ha rätt att föra ett ärende till dataombudsmannen även när någon i verksamhet som omfattas av den föreslagna lagens tillämpningsområde bryter mot sådana bestämmelser om behandling av personuppgifter som finns i speciallagstiftning och som ska tillämpas i verksamheten i fråga.

I personuppgiftslagen föreskrivs det inte uttryckligen om någon sådan allmän rätt för en registrerad att inleda ett ärende vid dataombudsmannens byrå. Enligt 40 § 2 mom. i personuppgiftslagen ska dataombudsmannen dock avgöra ett ärende som en registrerad med stöd av 28 § (utövande av rätten till insyn) och 29 § (rättelse av en uppgift) fört till denne för behandling. Dataombudsmannen kan bestämma att den registeransvarige ska se till att den registrerades rätt till insyn tillgodoses eller att en uppgift rättas. Enligt personuppgiftslagen kan den registrerade inte inleda ett ärende heller i datasekretessnämnden. Den föreslagna bestämmelsen innebär således en betydande utvidgning av de rättsmedel en registrerad har till sitt förfogande.

Enligt det föreslagna momentet kan en registrerad framställa en begäran om åtgärder i vilken situation som helst där han eller hon anser att någon vid behandlingen av hans eller hennes personuppgifter bryter mot bestämmelserna om behandling av personuppgifter. En begäran om åtgärder kan t.ex. gälla den registrerades rätt till insyn, rätt att få uppgifter rättade eller lagligheten i grunden för behandlingen. På anförande av besvär iakttas förvaltningslagens bestämmelser om hur ett ärende inleds.

Enligt andra meningen i momentet får ärendet med den registrerades samtycke föras till dataombudsmannen också av ett allmännyttigt samfund som främjar skyddet av personuppgifter. Ett sådant allmännyttigt samfund som främjar skyddet av personuppgifter kan företräda flera registrerade i ett ärende riktat till dataombudsmannen som gäller en begäran om åtgärder. Bestämmelsen begränsar t.ex. inte den registrerades möjligheter att anlita ombud när den registrerade lägger fram en begäran om åtgärder för dataombudsmannen.

Den föreslagna bestämmelsen grundar sig på artikel 55 i dataskyddsdirektivet, enligt vilken medlemsstaterna i enlighet med deras nationella processrätt ska se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte som har inrättats på lämpligt sätt och vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter vad gäller skyddet av deras personuppgifter, i uppdrag att lämna in en begäran om åtgärder för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

57 §. *Behandlingen av en begäran om åtgärder*. Paragrafen innehåller bestämmelser om behandling av en sådan begäran om åtgärder som avses i 56 §.

Genom paragrafens *1 mom.* genomförs artikel 46.1 f samt artikel 52.4 i dataskyddsdirektivet. Dataombudsmannen ska pröva ärendet, om inte ärendet är anhängigt i domstol. På handläggningen av ärendet tillämpas förvaltningslagen som allmän lag. Enligt vad som föreskrivs i 23 § i förvaltningslagen ska dataombudsmannen behandla ärendet utan obefogat dröjsmål, och ska bl.a. besvara en parts förfrågningar om hur behandlingen framskrider. I andra meningen i 1 mom. tas det in kompletterande bestämmelser om att dataombudsmannen inom rimlig tid ska informera den som framställt begäran om hur behandlingen fortskrider, om behandlingen av ärendet fördröjs på grund av att en ytterligare utredning behövs eller av något annat skäl. Omständigheter av betydelse när rimlig tid bedöms är t.ex. ärendets art, komplexitet och omfattning.

I *2 mom.* föreskrivs det om situationer då dataombudsmannen i ett ärende som har inletts hos dataombudsmannen anser att det behöver utredas huruvida ett i 41 § 1 mom. 3 punkten avsett beslut av kommissionen om adekvat skyddsnivå är förenligt med dataskyddsdirektivet. I sådana situationer ska dataombudsmannen till denna del föra ärendet till en förvaltningsdomstol för avgörande. Förvaltningsdomstolen kan för sin del göra en begäran om förhandsavgörande hos EU-domstolen. På grund av att det förmodligen inte kommer att förekomma många sådana fall och på grund av den sakkunskap som behövs i ärendet bör fallen koncentreras till en

enda förvaltningsdomstol, och därför ska dataombudsmannen enligt bestämmelsen föra ärendet till Helsingfors förvaltningsdomstol för behandling. Bestämmelserna i momentet grundar sig inte direkt på dataskyddsdirektivet utan på EU-domstolens rättspraxis och i synnerhet förhandsavgörandet i målet Schrems (C-362/14).

58 §. *Ändringssökande*. Paragrafen innehåller bestämmelser om sökande av ändring. Genom paragrafen genomförs artikel 53.1 och 53.3 i dataskyddsdirektivet. Avsikten med dem är att trygga en persons rätt till effektiva rättsmedel mot den nationella tillsynsmyndigheten, dvs. dataombudsmannen.

I *1 mom.* föreskrivs det om rätt att överklaga dataombudsmannens beslut genom besvär. Enligt bestämmelsen får dataombudsmannens beslut överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen. Bestämmelsen motsvarar innehållsmässigt 45 § 1 mom. i personuppgiftslagen. Huruvida ett beslut av dataombudsmannen är överklagbart bestäms med stöd av förvaltningsprocesslagen.

Enligt *2 mom.* får besvär över förvaltningsdomstolens beslut anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Bestämmelsen motsvarar 45 § 2 mom. i personuppgiftslagen. I andra meningen i momentet föreskrivs det att även dataombudsmannen har rätt att söka ändring i förvaltningsdomstolens beslut. Rätt för dataskyddsmannen att söka ändring behövs i synnerhet för att säkerställa en enhetlig rättspraxis, även med beaktande av att dataombudsmannen är ledamot av Europeiska dataskyddsstyrelsen.

Enligt *3 mom.* får det i dataombudsmannens beslut bestämmas att beslutet ska iakttas trots ändringssökande, om inte besvärsmyndigheten bestämmer något annat. På så sätt säkerställs att dataombudsmannen har möjlighet att ingripa effektivt i synnerhet i sådan lagstridig behandling av personuppgifter som kan medföra en risk för den registrerades rättigheter. Även enligt 45 § 3 mom. i personuppgiftslagen kan det i datasekretessnämndens beslut, på motsvarande vis som i den föreslagna bestämmelsen, bestämmas att beslutet ska iakttas även om det överklagas.

10 kap. Särskilda bestämmelser

59 §. *Skadestånd*. Paragrafen innehåller bestämmelser om den personuppgiftsansvariges skyldighet att ersätta den registrerade eller någon annan person för ekonomiska skada och annan skada som denne har tillfogats av att personuppgifter har behandlats i strid med lag. Artikel 56 i dataskyddsdirektivet ålägger medlemsstaterna att föreskriva att var och en som lidit materiell eller immateriell skada till följd av en olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de nationella bestämmelser som antas i enlighet med direktivet ska ha rätt till ersättning för denna skada från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Enligt *1 mom.* är den personuppgiftsansvarige skyldig att ersätta den registrerade eller någon annan person för ekonomisk skada och annan skada som denne tillfogats av att personuppgifter har behandlats i strid med denna lag. På samma sätt som för närvarande ska ersättningsansvaret således gälla ersättning för skada som tillfogats också någon annan person än den registrerade. Enligt bestämmelsen är det alltid den personuppgiftsansvarige som bär ersättningsansvaret.

I de föreslagna bestämmelserna kvarstår det skadeståndsansvar oberoende av vållande som ingår i 47 § i den gällande personuppgiftslagen. På samma sätt som för närvarande ska enligt paragrafen t.ex. sådan ekonomisk skada ersättas som den registrerade tillfogats på grund av att oriktiga uppgifter använts eller uppgifter lämnats ut i strid med lag. Ansvaret ska gälla också

ekonomisk och annan skada som förorsakats av all annan olaglig behandling av personuppgifter. På sätt täcker ansvaret också lidande som förorsakats en person av att personuppgifter behandlats olagligt.

Paragrafens *2 mom.* är informativt. Enligt det finns bestämmelser i övrigt om rätten till skadestånd i skadeståndslagen.

60 §. *Straffbestämmelser*. Det föreslås att det i paragrafen tas in en hänvisningsbestämmelse till de bestämmelser i strafflagen som kan komma i fråga som påföljder för överträdelser av lagen. I artikel 57 i dataskyddsdirektivet förutsätts att det föreskrivs om dem.

Paragrafen innehåller en hänvisningsbestämmelse till 38 kap. 9 § i strafflagen där det ska föreskrivas om dataskyddsbrott. En ny straffbestämmelse om dataskyddsbrott, genom vilken gällande straffbestämmelse om personregisterbrott upphävs, ingår i regeringens proposition med förslag till dataskyddslag.

I paragrafen hänvisas det också på samma sätt som i 48 § i personuppgiftslagen till 38 kap. 3, 4, 8 och 8 a § i strafflagen där det föreskrivs om straff för kränkning av kommunikationshemlighet och för grov kränkning av kommunikationshemlighet samt för dataintrång och för grovt dataintrång. Till straff för brott mot de föreslagna bestämmelserna om tystnadsplikt i 61 § döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte gärningen utgör brott enligt 40 kap.5 § i den lagen eller om inte strängare straff för den föreskrivs någon annanstans i lag.

61 §. *Tystnadsplikt*. Paragrafen innehåller bestämmelser om tystnadsplikt för den som deltagit i behandlingen av personuppgifter. Den som har deltagit i behandlingen av personuppgifter får inte obehörigen för utomstående röja de uppgifter som han eller hon erhållit på detta sätt eller använda uppgifterna för sin egen eller någon annans vinning eller för att skada någon annan. Den som deltar i behandlingen av personuppgifter kan bl.a. vara en person som är anställd hos den personuppgiftsansvarige eller den behöriga myndigheten, ett dataskyddsombud eller en person som behandlar personuppgifter för den personuppgiftsansvariges räkning.

En tystnadspliktsbestämmelse med motsvarande innehåll ingår i 33 § i den gällande personuppgiftslagen där det sägs att den som vid utförandet av åtgärder som har samband med behandlingen av personuppgifter har fått kännedom om något som gäller en annan persons egenskaper, personliga förhållanden eller ekonomiska ställning, inte i strid med personuppgiftslagen för tredje man får röja de uppgifter som han på detta sätt har erhållit. En motsvarande paragraf ingår också i den föreslagna dataskyddslagen.

11 kap. Ikraftträdande och övergångsbestämmelser

62 §. *Ikraftträdande*. Paragrafen innefattar en sedvanlig ikraftträdandebestämmelse. Enligt artikel 63.1 i dataskyddsdirektivet ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa direktivet. Medlemsstaterna ska också tillämpa dessa bestämmelser från och med nämnda dag.

63 §. *Övergångsbestämmelser*. I *1 mom.* tas det in en övergångsbestämmelse enligt vilken automatiserade behandlingssystem som har inrättats före den 6 maj 2016 i kan bringas i överensstämmelse med den föreslagna 19 § senast den 6 maj 2023.

Övergångsbestämmelsen grundar sig på artikel 63.2 i dataskyddsdirektivet. Övergångsbestämmelsen inverkar inte på automatiserade behandlingssystem som har inrättats efter den 6 maj 2016, vilka till alla delar ska bringas i överensstämmelser med den föreslagna lagen senast den 6 maj 2018.

1.2 Straffregisterlagen

1 §. Det föreslås att ordalydelsen i *1 mom.* preciseras så att där uttryckligen konstateras att Rättsregistercentralen är personuppgiftsansvarig i fråga om straffregistret. På Rättsregistercentralen påförs således för straffregistrets del de skyldigheter som den personuppgiftsansvarige har enligt den föreslagna allmänna lagen. Enligt den gällande straffregisterlagen förs straffregister vid Rättsregistercentralen enligt vad som bestäms i den lagen.

6 §. I 6 § *8 mom.* i straffregisterlagen föreslås det för det första att bestämmelserna om den registrerades kontrollrätt ska strykas. Det ska föreskrivas om saken i den föreslagna allmänna lagen. De bestämmelser som för närvarande ingår i momentet när det gäller rätten att få ett utdrag ur straffregistret om en juridisk person ses över så att det av ordalydelsen klarare framgår att det inte är fråga om den registrerades kontrollrätt. Ändringen är av teknisk natur.

1.3 Lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen

4 §. *Förhållande till andra lagar och internationella förpliktelser*. Det föreslås att 3 mom. ändras så att där inte längre hänvisas till personuppgiftslagen, som upphävs, utan till den allmänna lag som föreslås i denna proposition (lagförslag 1).

8 §. *Lagringsregistrets syfte*. Ordalydelsen i första meningen i paragrafen ses över så att Rättsregistercentralens roll som personuppgiftsansvarig för lagringsregistret framgår klarare. I övrigt kvarstår paragrafen oförändrad.

13 §. *Rätt till insyn*. Det föreslås att paragrafens bestämmelser om kontrollrätt ersätts med en informativ bestämmelse, enligt vilken det i fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt.

1.4 Lagen om justitieförvaltningens riksomfattande informationssystem

2 §. *Förhållande till annan lagstiftning*. Det föreslås att *1 mom.* ändras så att där inte längre hänvisas till personuppgiftslagen, som upphävs, utan till allmänna dataskyddsförordningen, dataskyddslagen samt den allmänna lag som föreslås i denna proposition (lagförslag 1).

7 §. Det föreslås att den svenska språkdräkten i 7 § *1 mom*. och *3 mom. 3 punkten* ändras så att termen ”registeransvarig” ersätts med termen ”personuppgiftsansvarig”. Momenten kvarstår i övrigt oförändrade.

10 §. *Personuppgifter som ska registreras i informationssystemet*. Det föreslås att *2 mom.* ändras så att hänvisningen till definitionen av känsliga uppgifter i personuppgiftslagen, som upphävs, ersätts med en hänvisning till artikel 9 i allmänna dataskyddsförordningen och till den definition av särskilda kategorier av personuppgifter som föreslås i 11 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

18 §. *Gallring av uppgifter*. Det föreslås att *2 mom.* upphävs. I momentet föreskrivs det för närvarande om gallring av uppgifter ur rapporterings-, statistik- och arkivsystemet enligt vad som föreskrivs i personuppgiftslagen. Avsikten är att upphäva personuppgiftslagen och ef-

tersom bestämmelser om dessa frågor kommer att tas in i de allmänna lagarna om behandling av personuppgifter, kan momentet upphävas i sin helhet.

19 §. *Rätt till insyn och rättelse av uppgifter*. Bestämmelserna om rätten till insyn och rättelse av uppgifter ersätts med en informativ bestämmelse, enligt vilken det i fråga om den registrerades rätt till insyn och rätt att få sina uppgifter rättade eller kompletterade förskrivs särskilt.

1.5 Lagen om verkställighet av böter

46 §. *Ändamålet med bötesregistret och behandlingen av registeruppgifterna*. Det föreslås att den svenska språkdräkten i *1 mom.* ändras så att termen ”registeransvarig” ersätts med termen ”personuppgiftsansvarig”. Paragrafens 1 och *2 mom.* kvarstår i övrigt oförändrade.

Det föreslås att *3 mom.* ändras så att den nuvarande informativa hänvisningen till personuppgiftslagen, som upphävs, ersätts med en informativ hänvisning till allmänna dataskyddsförordningen, dataskyddslagen och den allmänna lag som föreslås i denna proposition.

48 §. *Den personuppgiftsansvariges rätt att få uppgifter*. Det föreslås att den svenska språkdräkten ändras så att termen ”registeransvarig” ersätts med termen ”personuppgiftsansvarig”. Samtidigt ändras hänvisningen till centrala befolkningsregistret i paragrafen till befolkningsdatasystemet i enlighet med den gällande lagstiftningen om saken.

49 §. *Ansvaret för uppgifterna i bötesregistret*. Det föreslås att bestämmelserna om den registeransvariges skadeståndsansvar och övriga ansvar upphävs, eftersom bestämmelser om dessa omständigheter tas i den allmänna lagstiftning som blir tillämplig.

50 §. *Hemlighållande och utlämnande av uppgifter som ingår i bötesregistret*. Det föreslås att den svenska språkdräkten i *1 mom.* ändras så att termen ”registeransvarig” ersätts med termen ”personuppgiftsansvarig”. Momentet kvarstår i övrigt oförändrat.

1.6 Lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten

1 §. *Lagens tillämpningsområde*. Det föreslås att hänvisningsbestämmelsen i 1 mom. till personuppgiftslagen ersätts med en hänvisning till allmänna dataskyddsförordningen, dataskyddslagen och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten.

30 §. *Information om behandling av uppgifter*. Det föreslås att den hänvisningsbestämmelse som gäller personuppgiftslagen ändras till en hänvisning till allmänna dataskyddsförordningen och dataskyddslagen.

31 §. *Inskränkningar i rätten till insyn*. Det föreslås att hänvisningen i *1 mom.* till personuppgiftslagen ändras så att den överensstämmer med den nya personuppgiftslagstiftningen.

33 §. *Bevaring av uppgifter som konstaterats vara oriktiga*. Det föreslås att hänvisningen i 1 mom. till personuppgiftslagen ersätts med en hänvisning till den nya personuppgiftslagstiftningen.

37 §. *Straffbestämmelser*. I första meningen i *2 mom.* hänvisas det för närvarande till strafflagens bestämmelser om personregisterbrott och dataintrång i personregister. I den regeringsproposition som gäller ny dataskyddslag föreslås det att personregisterbrott ersätts med en straffbestämmelse om dataskyddsbrott. Denna begreppsändring görs också i det aktuella 2 mom. Enligt sista meningen i det gällande momentet döms till straff för personregisterförse-

else enligt 48 § 2 mom. i personuppgiftslagen. I dataskyddslagen tas det inte in bestämmelser om dataskyddsförseelse och hänvisningsbestämmelsen i fråga ska därför strykas.

Dessutom föreslås det att den svenska språkdräkten i lagens 11 §, 24 § 2 mom. 28 § 3 mom., 32 § och 34 § 3 mom. ändras så att termen ”registeransvarig” ersätts med termen ”personuppgiftsansvarig”. Nämnda bestämmelser kvarstår i övrigt oförändrade.

2 Ikraftträdande

Enligt artikel 63.1 i dataskyddsdirektivet ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa direktivet. De ska också tillämpa dessa bestämmelser från och med den 6 maj 2018. Av den anledningen föreslås det att lagarna ska träda i kraft den 6 maj 2018, ,eller så snart som möjligt efter det.

Det är dock möjligt att bringa automatiserade behandlingssystem som har inrättats före den 6 maj 2016 i överensstämmelse med den föreslagna 19 § senast den 6 maj 2023. Den föreslagna övergångsbestämmelsen grundar sig på artikel 63.2 i dataskyddsdirektivet. Enligt artikel 63.3 i dataskyddsdirektivet får en medlemsstat under exceptionella omständigheter, om fullgörandet av den loggningsskyldighet som anges i artikel 19 annars skulle medföra allvarliga problem för driften av detta specifika automatiserade behandlingssystem, förlänga övergångsperioden till denna del till den 6 maj 2026. Behovet av att utnyttja den extra flexibilitet som direktivet möjliggör ska vid behov bedömas närmare tidsfristen för den övergångsperiod som föreslås i denna proposition.

3 Förhållande till grundlagen samt lagstiftningsordning

3.1 Skydd för personuppgifter

De bestämmelser som föreslås i propositionen är viktiga med tanke på det i 10 § i grundlagen tryggade skyddet för privatlivet och personuppgifter. De föreslagna bestämmelserna konkretiserar dessa grundlagsbestämmelser på sitt tillämpningsområde och tryggar till denna del tillgodoseendet av de grundläggande och mänskliga rättigheterna på det sätt som förutsätts i 22 § i grundlagen.

De föreslagna bestämmelserna är betydelsefulla också t.ex. med tanke på Europeiska unionens stadga om de grundläggande rättigheterna. I artikel 7 i stadgan tryggas respekten för privatlivet och i artikel 8 vars och ens rätt till skydd av de personuppgifter som rör honom eller henne. Enligt artikeln ska dessa uppgifter behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. I EU-domstolens domar fastställs till denna del det centrala innehållet i respekten för privatlivet och skyddet för personuppgifter. Artikel 8 om rätten till skydd för privat- och familjeliv i Europakonventionen har i Europadomstolens rättspraxis ansetts omfatta även skyddet för personuppgifter.

I och med förslaget genomförs EU:s dataskyddsdirektiv nationellt. Grundlagsutskottet ansåg i sitt utlåtande om förslaget till direktiv att förslaget till sitt materiella innehåll rätt väl följer och konkretiserar bestämmelserna om skydd för personuppgifter i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Grundlagsutskottet ansåg vidare att förslaget inte var problematiskt heller med utgångpunkt i 10 § 1 mom. i grundlagen och utskottets preciserande praxis (GrUU 12/2012 rd).

Enligt bestämmelserna i artikel 1.3 i direktivet ska direktivet inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet för skyddet av den regi-

strerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter. I den allmänna lag som föreslås i denna proposition har det därför tagits in vissa förslag till bestämmelser som tillgodoser de registrerades rättigheter bättre än vad som förutsätts i direktivet, bl.a. när det gäller behandlingen av personbeteckningar samt uppgifter som ska ingå i en dataskyddsbeskrivning som ska göras allmänt tillgänglig.

I sin bedömning av bestämmelserna om skydd för personuppgifter har grundlagsutskottet ansett att sådana bestämmelser måste granskas mot 10 § i grundlagen. Enligt den paragrafens 1 mom. 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 skyddet för privatlivet som tryggas i samma moment. 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 över lag (bl.a. GrUU 2/2018 rd, GrUU 31/2017 rd, GrUU 5/2017 rd).

Om man ser till skyddet för personuppgifter har grundlagsutskottet ansett det viktigt att reglera åtminstone syftet med registreringen av uppgifterna, uppgifternas innehåll, det tillåtna användningsändamålet inklusive rätten att överlåta registrerade uppgifter, den tid uppgifterna finns kvar i registret och den registrerades rättsskydd. Dessutom ska regleringen av dessa faktorer på lagnivå vara heltäckande och detaljerad (se t.ex. GrUU 2/2018 rd, GrUU 31/2017 rd, GrUU 28/2016, GrUU 13/2016 rd). Med tanke på den föreslagna allmänna lagen (lagförslag 1) är det väsentligt att det enligt grundlagsutskottets uppfattning inte finns något hinder för att kraven på räckvidd för, exakthet hos och noggrann avgränsning av bestämmelser om skyddet av personuppgifter till vissa delar kan uppfyllas genom en allmän nationell lag (bl.a. GrUU 2/2018 rd, GrUU 1/2018 rd, GrUU 31/2017 rd, GrUU 5/2017 rd).

I artikel 8.2 i dataskyddsdirektivet förutsätts att medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för direktivet åtminstone ska specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål. Enligt den precisering som ges i skäl 33 i ingressen innebär en hänvisning till medlemsstaternas nationella rätt inte enbart en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den berörda medlemsstatens konstitutionella ordning.

Den föreslagna allmänna lagen ska tillämpas på sådan behandling av personuppgifter som sker i samband med brottmål. Den ska tillämpas också på sådan behandling av personuppgifter som utförs av Försvarsmakten, Gränsbevakningsväsendet och polisen i samband med upprätthållandet av den nationella säkerheten. Avsikten är att den föreslagna allmänna lagen ska kompletteras med speciallagstiftning för de olika förvaltningsområdena. Speciallagstiftningen ska i behövlig utsträckning innehålla närmare bestämmelser t.ex. om vilka personuppgifter som registreras, deras användningsändamål, utlämnande av personuppgifter och hur länge uppgifterna bevaras. Den lagstiftning som ska tillämpas ska granskas som en helhet, och strävan har därför varit att bereda de propositioner som gäller saken parallellt så långt det varit möjligt.

I den allmänna lagen ska det tas in bestämmelser om de allmänna förutsättningarna för behandling av personuppgifter, såsom krav på laglig behandling, ändamålsbegränsning, relevanskrav, felfrihetskrav, åtskillnad mellan olika personuppgifter och behandling av personbeteckningar. En allmän förutsättning för behandling av personuppgifter är att behandlingen behövs för att en behörig myndighet ska kunna utföra en uppgift på den föreslagna lagens tillämpningsområde, och att det föreskrivs om behandlingen i lag, antingen i nationell lag eller i EU-lagstiftningen.

I lagen ska det också tas in bestämmelser om förutsättningarna för behandling av särskilda personuppgifter (s.k. känsliga uppgifter). Grundlagsutskottet har i sin tolkningspraxis fäst uppmärksamhet vid de hot som behandlingen av sådana personuppgifter medför. Enligt utskottet föranleder exempelvis registreringen av biometriska kännetecken, som anses utgöra känsliga uppgifter, ett särskilt behov att se till att de personuppgifter som sparas i systemet blir skyddade mot risker för missbruk och mot alla slag av olaglig åtkomst och användning (GrUU 1/2018 rd, GrUU 13/2017 rd, GrUU 29/2016 rd). Utskottet har särskilt påpekat att det bör finnas exakta och noga avgränsade bestämmelser om att det är tillåtet att behandla känsliga uppgifter bara om det är absolut nödvändigt (se t.ex. GrUU 1/2018 rd, GrUU 13/2017 rd och GrUU 3/2017 rd). Den föreslagna allmänna lagen ska därför innehålla bestämmelser om att känsliga personuppgifter får behandlas endast på vissa i lag angivna villkor och endast om det är nödvändigt. En förutsättning för att behandla känsliga uppgifter är också att de skyddsåtgärder som krävs för att trygga den registrerades rättigheter har vidtagits.

I den föreslagna allmänna lagen tas det också in bestämmelser om den personuppgiftsansvariges och personuppgiftsbiträdets ansvar, såsom skyldigheten att bevara logguppgifter över insamling, ändring och läsning av personuppgifter som utförts i ett automatiserat behandlingssystem. Den personuppgiftsansvarige ska innan behandlingen av personuppgifter inleds göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter samt på vissa villkor höra dataombudsmannen om den planerade behandlingen.

I den föreslagna allmänna lagen tas det in bestämmelser också om de registrerades rätt till insyn och rätt att få personuppgifter rättade eller utplånade samt bestämmelser om begränsning av ovannämnda rättigheter för de registrerade. Registrerade personer ska ha rätt att lämna in en begäran om åtgärder till den som utövar tillsyn över efterlevnaden av den föreslagna lagen, dvs. dataombudsmannen, om de registrerade anser att behandling som avser dem står i strid med den föreslagna lagen. Dataombudsmannen ska t.ex. ha möjlighet att ge den personuppgiftsansvarige en anmärkning eller bestämma att personuppgifter ska rättas eller behandlingen begränsas, och kan vid behov förena ett rättsligt bindande beslut med vite.

I lagen tas det också in detaljerade bestämmelser om informationssäkerhet samt bestämmelser om kravet att utnämna ett dataskyddsombud.

Lagen ska också innehålla bestämmelser om de detaljerade förutsättningarna för att få överföra personuppgifter till tredjeländer eller internationella organisationer. Grundlagsutskottet har ansett det viktigt att reglera utlämnandet av personuppgifter med tanke på skyddet av personuppgifter. Grundlagsutskottet har ansett det möjligt att lämna ut uppgifter till tredjeländer och då fäst särskild uppmärksamhet vid nivån på skyddet av personuppgifter i landet i fråga, en godtagbar grund för utlämnande av personuppgifterna samt en lämplig avgränsning av möjligheten att lämna ut uppgifter (bl.a. GrUU 21/2017 rd, GrUU 13/2017 rd, GrUU 20/2016), även om det i vissa regleringssammanhang i princip förhållit sig negativt till utlämnande av personuppgifter till tredjeländer (GrUU 28/2016 rd, GrUU 21/2012 rd). Vid behandlingen av förslaget till ett EU-system för reseuppgifter och resetillstånd ansåg utskottet det möjligt ur konstitutionell synpunkt att lämna ut uppgifter till tredjeländer i samband med återsändande av dessa länders medborgare eller i exceptionella nödsituationer, när syftet är att bekämpa terrorism eller annan allvarlig brottslighet (GrUU 21/2017 rd). Utskottet har i vissa av sina utlåtanden understrukit att en förutsättning för ett utlämnande till utlandet bör vara att utlämnandet av uppgifterna är ”nödvändigt” för något ändamål, om det datainnehåll som utlämnas inte har uppräknats på ett uttömmande sätt (bl.a. GrUU 51/2002 rd, GrUU 14/2002 rd).

I 7 kap. i den föreslagna allmänna lagen (lagförslag 1) föreskrivs om överföring av personuppgifter till tredjeländer och internationella organisationer. I fråga om det mottagande landet ska det i princip finnas ett beslut av kommissionen om att dataskyddsnivån i landet är adekvat.

I artikel 36 i dataskyddsdirektivet föreskrivs det om de omständigheter som kommissionen ska beakta när den gör bedömningen. Dessa omständigheter omfattar bl.a. rättsstatsprincipen, effektiv administrativ och rättslig prövning, oberoende tillsyn över efterlevnaden av dataskyddsbestämmelserna samt de internationella överenskommelser om saken där staten är part. Om kommissionen inte har fattat beslut om adekvat skyddsnivå för staten i fråga, är en överföring enligt den föreslagna lagen möjlig också om skyddet av personuppgifter har tryggats genom bilaterala överenskommelser eller på något annat sätt. I undantagsfall får personuppgifter överföras också om överföringen är nödvändig t.ex. för att skydda intressen som är av grundläggande betydelse för en fysisk person eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en stat. De föreslagna bestämmelserna grundar sig på de bestämmelser om att föreskriva om saken i lag som finns i kapitel VI i dataskyddsdirektivet.

3.2 Förhållandet mellan offentlighetslagstiftningen och den föreslagna dataskyddslagstiftningen

Enligt 12 § 2 mom. i grundlagen är handlingar och upptagningar som innehas av myndigheterna offentliga, om inte offentligheten av tvingande skäl särskilt har begränsats genom lag. Var och en har rätt att ta del av offentliga handlingar och upptagningar. Grundlagsutskottet har ansett det viktigt med balans mellan skyddet av personuppgifter och offentliga handlingars offentlighet (bl.a. GrUU 60/2017 rd, GrUU 15/2017 rd, GrUU 12/2012 rd, GrUU 22/2008 rd). I den föreslagna allmänna lagen (lagförslag 1) tas det in en hänvisningsbestämmelse till lagstiftningen om offentlighet i myndigheternas verksamhet. Avsikten är inte att genom denna proposition ändra det nuvarande inbördes förhållandet mellan offentlighetslagstiftningen och lagstiftningen om skydd för personuppgifter.

3.3 Skydd för hemfriden

I 48 § i den föreslagna allmänna lagen finns en bestämmelse om en möjlighet för dataombudsmannen att göra inspektioner för att övervaka efterlevnaden av lagen. I utrymmen som används för boende av permanent natur får inspektion utföras endast om det är nödvändigt för att utreda de omständigheter som är föremål för inspektion och det finns motiverade och specificerade skäl att misstänka att det har skett eller kommer att ske en sådan överträdelse av bestämmelserna om behandling av personuppgifter att påföljden kan vara ett straff enligt strafflagen.

Vars och ens privatliv är tryggat enligt 10 § 1 mom. i grundlagen. Genom lag kan med stöd av 10 § 3 mom. i grundlagen bestämmas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas eller för att brott ska kunna utredas. Med tanke på principen om regleringens proportionalitet har grundlagsutskottet utgått från att man inte bör ingripa i skyddet för hemfriden för att utreda föga klandervärda förseelser som allra högst bestraffas med böter (bl.a. GrUU 2/2017 rd, GrUU 40/2002 rd). De föreslagna bestämmelserna om inspektion har på det sätt som grundlagsutskottet förutsatt knutits till en nödvändighetsförutsättning samt till en motiverad och specificerad misstanke om ett förfarande som är straffbart enligt strafflagen. Utöver detta kan en inspektion i praktiken bli aktuell endast för utredning av gärningar som är straffbara enligt strafflagen och till vilka de hänvisas i 60 § i den föreslagna allmänna lagen.

Vid inspektioner ska förvaltningslagens 39 § iakttas. Bestämmelserna uppfyller även till denna del kraven i grundlagsutskottets praxis (GrUU 44/2016 rd, GrUU 11/2013 rd).

Enligt det föreslagna 50 § 2 mom. får dataombudsmannen vid inspektioner anlita biträde av utomstående sakkunniga. Enligt 124 § i grundlagen får uppgifter som innebär betydande utövning av offentlig makt ges endast myndigheter. Som betydande utövning av offentlig makt be-

traktas t.ex. på självständig prövning baserad rätt att använda maktmedel eller att på något annat konkret sätt ingripa i en enskild persons grundläggande fri- och rättigheter (RP 1/1998 rd, s. 180, GrUU 28/2001 rd). Grundlagsutskottet har i sin praxis ansett att befogenhet att utföra inspektioner på hemfridsskyddade platser innebär rätt till ett betydande ingrepp i vars och ens grundlagstryggade hemfrid och att en enskild därmed inte kan få en sådan befogenhet genom en vanlig lag (se GrUU 40/2002 rd och GrUU 46/2001 rd). Däremot är det ingenting som hindrar att man föreskriver att en person som utsetts utom myndighetsmaskineriet har rätt att bistå övervakaren i åtgärder som ingriper i hemfriden (t.ex. GrUU 44/2016 rd och GrUU 30/2010 rd). En sådan utomstående sakkunnig som avses i de föreslagna bestämmelserna ska inte få utföra inspektion självständigt, utan den sakkunnige har alltid en assisterande uppgift i förhållande till dataombudsmannen.

3.4 Tillsyn över efterlevnaden av lagen och rättsmedel

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.

Dataombudsmannen ska utöva tillsyn över efterlevnaden av den föreslagna lagen. Dataombudsmannen ska vara självständig och oberoende i sin verksamhet. Dataombudsmannen ska behandla begäranden om åtgärder från registrerade och kunna meddela beslut som är bindande för den personuppgiftsansvarige eller personuppgiftsbiträdet. Dataombudsmannen ska vid behov kunna förena besluten med vite. Dataombudsmannens beslut får överklagas genom besvär hos förvaltningsdomstolen på det sätt som föreskrivs i förvaltningsprocesslagen.

I den föreslagna allmänna lagen tas det in bestämmelser om rätt till ersättning för den registrerade eller någon annan person för sådan skada som tillfogats denne av att personuppgifter har behandlats i strid med lag. Den registrerade ska ha rätt att av den personuppgiftsansvarige få ersättning för den ekonomiska skada eller annan skada som tillfogats honom eller henne av att personuppgifter har behandlats i strid med den föreslagna lagen. Det är fråga om ett ur den personuppgiftsansvariges synvinkel s.k. strikt skadeståndsansvar oberoende av oaktsamhet.

I ärenden som omfattas av den föreslagna lagens tillämpningsområde ska dataombudsmannen dock inte övervaka domstolarnas, justitiekanslerns eller justitieombudsmannens verksamhet, vilket beror på deras konstitutionella ställning. Justitiekanslern och justitieombudsmannen ska övervaka dataombudsmannens verksamhet som en del av sina uppgifter som laglighetsövervakare. De ska också övervaka sådan behandling av personuppgifter som domstolarna utför i samband med sina rättskipningsuppgifter, även om det inte föreslås att tillsynen över domstolarnas verksamhet ska ingå i dataombudsmannens behörighet.

3.5 Slutsats

De lagförslag som ingår i propositionen kan enligt regeringens åsikt behandlas i vanlig lagstiftningsordning. De bestämmelser som föreslås i propositionen är som helhet sett betydelsefulla i konstitutionellt hänseende med tanke på skyddet för privatlivet och skyddet av personuppgifter enligt 10 § i grundlagen, och bestämmelserna tangerar också andra grundläggande fri- och rättigheter. Enligt regeringens uppfattning bör propositionen av dessa orsaker sändas till riksdagens grundlagsutskott för behandling.

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

Lagförslag

1.

Lag

om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

Denna lag tillämpas vid sådan behandling av personuppgifter som utförs av behöriga myndigheter när det är fråga om

1) förebyggande, avslöjande och utredning av brott eller förande av brott till åtalsprövning,

2) åtalsprövning och annan åklagarverksamhet som har samband med brott,

3) handläggning av brottmål i domstol,

4) verkställighet av straffrättsliga påföljder,

5) skydd mot eller förhindrande av hot mot den allmänna säkerheten i samband med verksamhet som avses i 1—4 punkten.

Utöver vad som föreskrivs i 1 mom. tillämpas denna lag på

1) sådan behandling av personuppgifter som utförs av Försvarsmakten och för Försvarsmaktens räkning, när uppgifterna behandlas för skötsel av uppgifter som anges i 2 § 1 mom. 1 punkten, 2 punkten underpunkt a samt 3 och 4 punkten i lagen om försvarsmakten (551/2007),

2) sådan behandling av personuppgifter som utförs av polisen, när uppgifterna behandlas inom ramen för en i 1 § 1 mom. i polislagen (872/2011) avsedd uppgift som hänför sig till skyddet av den nationella säkerheten,

3) sådan behandling av personuppgifter som utförs av Gränsbevakningsväsendet, när uppgifterna behandlas inom ramen för en i 3 § 2 och 3 mom. i gränsbevakningslagen (578/2005) avsedd uppgift som hänför sig till skyddet av den nationella säkerheten.

På sådan behandling av personuppgifter som avses i 2 mom. tillämpas dock inte bestämmelserna i 10 § 2 mom. om överföring av personuppgifter till en mottagare inom Europeiska unionen, bestämmelserna i 54 § om ömsesidigt bistånd i fråga om andra medlemsstater i Europeiska unionen och bestämmelserna i 7 kap. om överföringar av personuppgifter till tredjeländer och internationella organisationer.

Denna lag tillämpas dock endast på sådan i 1 och 2 mom. avsedd behandling av personuppgifter som är helt eller delvis automatiserad eller där de uppgifter som behandlas utgör eller är avsedda att utgöra ett register eller en del av ett sådant.

Genom denna lag genomförs 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*.

2 §

Förhållande till annan lagstiftning

Om det i någon annan lag finns bestämmelser som avviker från denna lag, ska de tillämpas i stället för denna lag.

På rätten att få uppgifter ur myndigheternas personregister och på annat utlämnande av personuppgifter ur dessa personregister tillämpas vad som föreskrivs om offentlighet i myndigheternas verksamhet.

3 §

Definitioner

I denna lag avses med

1) *personuppgifter* varje upplysning som direkt eller indirekt avser en identifierad eller identifierbar fysisk person (*en registrerad*),

2) *behandling* insamling, registrering, organisering, strukturering, bevarande, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, utplåning eller förstöring samt någon annan åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter,

3) *begränsning av behandling* markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4) *register* en strukturerad samling av personuppgifter som är tillgängliga enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

5) *behörig myndighet* en myndighet som har behörighet att förebygga, avslöja eller utreda brott eller föra brott till åtalsprövning, att åtalspröva eller vidta andra åtgärder som avser åtal för brott eller att döma till straffrättsliga påföljder eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förhindra hot mot den allmänna säkerheten, samt Försvarsmakten, polisen och Gränsbevakningsväsendet när de sköter uppgifter som avses i 1 § 2 mom.,

6) *personuppgiftsansvarig* en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter eller som enligt lag har till uppgift att föra ett register,

7*) personuppgiftsbiträde* en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

8) *mottagare* en fysisk eller juridisk person, en myndighet, ett ämbetsverk eller något annat organ till vilket personuppgifterna lämnas ut,

9) p*ersonuppgiftsincident* en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

10) *lämpliga skyddsåtgärder* sådana tekniska och organisatoriska åtgärder som säkerställer att behandlingen av personuppgifter är lagenlig, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerades rättigheter,

11) *profilering* automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma personliga egenskaper hos en fysisk person,

12) *genetiska uppgifter* personuppgifter som rör sådana nedärvda eller förvärvade genetiska kännetecken för en fysisk person som ger unik information om personens fysiologi eller hälsa, och som härrör från en analys av ett biologiskt prov från personen i fråga eller som erhållits på annat sätt,

13) *biometriska uppgifter* personuppgifter som tagits fram genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av personen i fråga,

14) *uppgifter om hälsa* personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa och som ger information om personens hälsotillstånd,

15*) tredjeland* andra stater än medlemsstater i Europeiska unionen (EU), stater inom Europeiska ekonomiska samarbetsområdet eller Schweiz,

16) *internationell organisation* en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som har inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.

Vad som i denna lag föreskrivs om behörig myndighet tillämpas också på enskilda som sköter en uppgift som avses i 1 mom. 5 punkten.

Vad som i denna lag föreskrivs om en medlemsstat i EU tillämpas också på stater inom Europeiska ekonomiska samarbetsområdet och på Schweiz.

2 kap.

Principer för behandling av personuppgifter

4 §

Krav på laglig behandling

Personuppgifter får behandlas endast om det behövs för att en behörig myndighet ska kunna utföra en i lag angiven uppgift på ett område som anges i 1 § 1 eller 2 mom.

Personuppgifter ska behandlas på ett korrekt och omsorgsfullt sätt.

5 §

Ändamålsbegränsning

Den personuppgiftsansvarige får samla in personuppgifter endast för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandla dem på ett sätt som står i strid med dessa ändamål.

Personuppgifter som har samlats in för ett ändamål som anges i 1 § 1 eller 2 mom. får behandlas för något annat än ett i momentet angivet ändamål endast om det föreskrivs om behandlingen i lag.

Personuppgifter får behandlas i ett i 1 § 1 eller 2 mom. angivet syfte också för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål, om lämpliga skyddsåtgärder för de registrerades rättigheter har vidtagits.

6 §

Relevanskrav

De personuppgifter som behandlas ska vara adekvata och behövliga med hänsyn till ändamålet med behandlingen och får inte vara för omfattande i förhållande till de ändamål för vilka de behandlas. Obehövliga personuppgifter ska utplånas utan obefogat dröjsmål.

Personuppgifter får inte lagras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som behövs med hänsyn till ändamålet med behandlingen.

Behovet att bevara personuppgifter ska bedömas med minst fem års mellanrum, om inte något annat föreskrivs om bevaringstider för personuppgifter någon annanstans.

7 §

Felfrihetskrav

De personuppgifter som behandlas ska vara korrekta och vara uppdaterade med hänsyn till ändamålet med behandlingen. Den personuppgiftsansvarige ska se till att alla rimliga åtgärder har vidtagits för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas antingen utplånas eller rättas utan dröjsmål.

8 §

Åtskillnad mellan olika personuppgifter

Den personuppgiftsansvarige ska vid behov och så långt det är möjligt göra en klar åtskillnad mellan personuppgifter som avser registrerade i olika ställning med tanke på det ärende som behandlas.

Alla rimliga åtgärder ska vidtas för att skilja personuppgifter som grundar sig på fakta från personuppgifter som grundar sig på personliga bedömningar.

9 §

Säkerställande av kvaliteten på personuppgifter som överförs eller görs tillgängliga

Den behöriga myndigheten ska vidta alla rimliga åtgärder för att se till att personuppgifter som är oriktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga.

Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga, tillförlitliga och aktuella.

Om det visar sig att oriktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts, ska mottagaren utan dröjsmål informeras om detta. Efter att mottagaren informerats om saken ska denne rätta eller utplåna personuppgifterna eller begränsa behandlingen av dem.

10 §

Skyldighet att informera om särskilda förutsättningar för behandlingen

Om det i lag anges särskilda förutsättningar för behandling av personuppgifter, ska den behöriga myndigheten i samband med utlämnande eller överföring av personuppgifter informera mottagaren av personuppgifterna om dessa förutsättningar samt om skyldigheten att iaktta dem.

När den behöriga myndigheten överför personuppgifter till en mottagare inom EU får den inte uppställa strängare krav på behandlingen av personuppgifter än vad som tillämpas nationellt på likartade uppgiftsöverföringar.

11 §

Behandling av särskilda kategorier av personuppgifter

Uppgifter som hör till särskilda kategorier av personuppgifter är personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person samt uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Sådana personuppgifter som avses i 1 mom. får behandlas endast om det är nödvändigt och de skyddsåtgärder som krävs för att trygga den registrerades rättigheter har vidtagits och

1) det föreskrivs om behandlingen i lag,

2) det är fråga om handläggning av brottmål i åklagarverksamhet eller i domstol,

3) det krävs för att skydda ett intresse som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller

4) behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter är förbjuden.

12 §

Behandling av personbeteckningar

En personbeteckning får behandlas endast om det är viktigt att entydigt identifiera den registrerade

1) för att en behörig myndighet ska kunna utföra en i lag angiven uppgift,

2) för att tillgodose den registrerades eller den personuppgiftsansvariges rättigheter eller uppfylla den registrerades eller den personuppgiftsansvariges skyldigheter, eller

3) för sådan historisk eller vetenskaplig forskning eller sådan statistikföring som avses i 5 § 3 mom.

En personbeteckning får inte onödigtvis antecknas i handlingar som skrivs ut eller upprättas på basis av ett register.

13 §

Automatiserat individuellt beslutsfattande

Om inte något annat föreskrivs i lag, får ett beslut inte fattas enbart på grundval av automatiserad behandling av personuppgifter, om beslutet har negativa rättsverkningar för den registrerade eller beslutet annars är betydande för den registrerade.

3 kap.

Personuppgiftsansvarig och personuppgiftsbiträde

14 §

Den personuppgiftsansvariges ansvar

Den personuppgiftsansvarige svarar för att personuppgifter behandlas i enlighet med lag. Den personuppgiftsansvarige ska dessutom kunna visa att personuppgifterna har behandlats i enlighet med 2 kap.

Den personuppgiftsansvarige ska vidta de tekniska och organisatoriska åtgärder som krävs med avseende på ansvaret enligt 1 mom. När åtgärderna vidtas ska hänsyn tas till behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter.

15 §

Inbyggt dataskydd och dataskydd som standard

Den personuppgiftsansvarige ska vid tidpunkten för beslut om hur behandlingen av personuppgifter ska utföras och vid tidpunkten för själva behandlingen av personuppgifter genomföra lämpliga tekniska och organisatoriska skyddsåtgärder för att säkerställa att behandlingen är laglig och att den registrerades rättigheter skyddas. Åtgärderna ska vidtas med beaktande av tillgängliga tekniska lösningar, genomförandekostnaderna samt behandlingens art, omfattning, sammanhang och ändamål samt de risker som behandlingen medför för personens rättigheter.

Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att i standardfallet säkerställa att endast personuppgifter som behövs för varje specifikt ändamål med behandlingen behandlas.

16 §

Gemensamt personuppgiftsansvariga

Om två eller flera personuppgiftsansvariga gemensamt fastställer behandlingens ändamål och medel, ska de komma överens om den inbördes ansvarsfördelningen vid skötseln av skyldigheter enligt denna lag, om det inte föreskrivs om ansvarsfördelningen i lag.

Personuppgiftsansvariga som avses i 1 mom. ska inom sig utse en personuppgiftsansvarig som fungerar som kontaktpunkt och med vilken den registrerade kan ha kontakt i frågor som gäller utövandet av den registrerades rättigheter. Den registrerade får dock utöva sina rättigheter enligt denna lag i förhållande till var och en av de personuppgiftsansvariga.

17 §

Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning ska lämna den personuppgiftsansvarige lämpliga utredningar och förbindelser och även i övrigt tillräckliga garantier för de organisatoriska och tekniska åtgärder genom vilka det säkerställs att personuppgifterna behandlas i enlighet med kraven i denna lag.

Personuppgiftsbiträdet eller en anställd hos personuppgiftsbiträdet får inte behandla personuppgifter på ett sätt som avviker från den personuppgiftsansvariges instruktioner och inte överföra behandlingen av personuppgifter på något annat personuppgiftsbiträde utan skriftligt tillstånd av den personuppgiftsansvarige.

Den behandling av personuppgifter som personuppgiftsbiträdet utför ska regleras i ett skriftligt avtal eller i ett skriftligt förordnande, i vilket typen av personuppgifter, behandlingens varaktighet, art och ändamål, kategorierna av personuppgifter och kategorierna av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I ovannämnda skriftliga handling ska det dessutom bestämmas att personuppgiftsbiträdet

1) ska handla enbart enligt instruktioner från den personuppgiftsansvarige,

2) ska säkerställa att de fysiska personer som behandlar personuppgifterna har förbundit sig att iaktta sekretess eller att de omfattas av en lagstadgad tystnadsplikt,

3) på lämpligt sätt ska bistå den personuppgiftsansvarige för att säkerställa att de bestämmelser som gäller den registrerades rättigheter iakttas,
4) beroende på den personuppgiftsansvariges val, ska utplåna eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats, och utplåna befintliga kopior, om inte något annat föreskrivs i lag,
5) ska ge den personuppgiftsansvarige tillgång till all information som behövs för att visa att denna paragraf iakttas,
6) ska uppfylla de förutsättningar som avses i denna paragraf för anlitande av ett annat personuppgiftsbiträde.

18 §

Register över behandlingar

Den personuppgiftsansvarige ska föra ett skriftligt register över behandling av personuppgifter som utförts under dess ansvar. Registret ska innehålla följande uppgifter:
1) namn och kontaktuppgifter för den personuppgiftsansvarige och eventuella gemensamt personuppgiftsansvariga samt för det dataskyddsombud som avses i 38 §,
2) ändamålen med och den rättsliga grunden för behandlingen av personuppgifter,
3) en beskrivning av kategorin eller kategorierna av registrerade och av kategorierna av personuppgifter,
4) de kategorier av mottagare som personuppgifterna har lämnats ut till eller ska lämnas ut till,
5) kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation,
6) om möjligt, de planerade tidsfristerna för utplåning av de olika kategorierna av personuppgifter,
7) eventuell användning av profilering,
8) om möjligt, en allmän beskrivning av informationssystemen och principerna för skydd av dem samt en allmän beskrivning av de tekniska och organisatoriska skyddsåtgärder som avses i 31 §.

Personuppgiftsbiträdet ska föra ett skriftligt register över all behandling av personuppgifter som utförs för den personuppgiftsansvariges räkning. Registret ska innehålla följande uppgifter:
1) namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena samt för dataskyddsombudet,
2) namn och kontaktuppgifter för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar,
3) de kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning,
4) eventuella uppgifter om överföringar av personuppgifter till ett tredjeland eller en internationell organisation, om den personuppgiftsansvarige uttryckligen begär detta,
5) om möjligt, en allmän beskrivning av de tekniska och organisatoriska skyddsåtgärder som avses i 31 §.

19 §

Logguppgifter

Den personuppgiftsansvarige och personuppgiftsbiträdet ska se till att logguppgifter bevaras över insamling, ändring, läsning, utlämnande, överföring, sammanförande och utplåning av personuppgifter som utförts i deras automatiserade behandlingssystem. De logguppgifter som gäller läsning och utlämnande ska göra det möjligt att utreda grund, datum och tidpunkt för

läsning och utlämnande och i möjligaste mån vem som har läst eller lämnat ut personuppgifterna samt mottagarnas identitet.

Logguppgifterna får användas endast för att kontrollera om behandlingen är lagenlig, för intern kontroll, för att säkerställa personuppgifternas integritet och säkerhet samt inom ramen för straffrättsliga förfaranden.

20 §

Konsekvensbedömning avseende dataskydd

Den personuppgiftsansvarige ska innan behandlingen av personuppgifter inleds göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Den personuppgiftsansvarige ska göra en skriftlig konsekvensbedömning, om den planerade behandlingen av personuppgifter kan medföra en betydande risk för tillgodoseendet av fysiska personers rättigheter. Konsekvensbedömningen ska innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för den registrerades rättigheter och åtgärder för att minska dem samt åtgärder för att säkerställa skyddet av personuppgifter.

21 §

Förhandssamråd med dataskyddsmyndigheten

Den personuppgiftsansvarige eller personuppgiftsbiträdet ska höra dataombudsmannen innan personuppgifterna behandlas, om

1) den skriftliga konsekvensbedömning som avses i 20 § 2 mom. visar att behandlingen trots planerade skyddsåtgärder medför en betydande risk för de registrerades rättigheter, eller

2) behandlingen av uppgifter särskilt vid användning av ny teknik eller nya rutiner eller förfaranden medför en betydande risk för de registrerades rättigheter.

Den personuppgiftsansvarige ska till dataombudsmannen lämna in en sådan konsekvensbedömning som avses i 20 § 2 mom. och på begäran andra sådana uppgifter som gör att dataombudsmannen kan bedöma lagligheten i behandlingen av personuppgifter.

Om dataombudsmannen anser att den behandling som avses i 1 mom. skulle stå i strid med denna lag, ska dataombudsmannen inom sex veckor från det att begäran om samråd mottogs ge den personuppgiftsansvarige och ett eventuellt personuppgiftsbiträde handledning i syfte att göra behandlingen lagenlig. Denna period får förlängas med en månad om den planerade behandlingen är så komplicerad att en förlängning krävs. Dataombudsmannen ska inom en månad från det att begäran om samråd mottogs informera den personuppgiftsansvarige och ett eventuellt personuppgiftsbiträde om den förlängda perioden och om skälen till fördröjningen.

4 kap.

De registrerades rättigheter

22 §

Dataskyddsbeskrivning och skyldighet att informera

Den personuppgiftsansvarige ska tillhandahålla en aktuell skriftlig beskrivning av sådan behandling av personuppgifter som denne ansvarar för. Beskrivningen ska göras offentligt tillgänglig och innehålla åtminstone följande uppgifter:

1) kontaktuppgifter för den personuppgiftsansvarige och dataskyddsombudet samt, om den personuppgiftsansvarige anser det behövligt, dataskyddsombudets namn,

2) namn och kontaktuppgifter för den personuppgiftsansvariga som fungerar som kontaktpunkt för gemensamt personuppgiftsansvariga samt uppgift om att den registrerade kan utöva sina rättigheter enligt denna lag i förhållande till var och en av de personuppgiftsansvariga,
3) ändamålen med och den rättsliga grunden för behandlingen av personuppgifter,
4) den period under vilken personuppgifterna kommer att bevaras eller, om den inte har fastställts, kriterierna för att fastställa denna period,
5) eventuella sedvanliga mottagare eller kategorier av mottagare av personuppgifterna,
6) uppgift om den registrerades rätt att av den personuppgiftsansvarige begära tillgång till personuppgifter som rör den registrerade samt rätt att begära att personuppgifterna rättas eller utplånas eller att behandlingen av dem begränsas,
7) uppgift om den registrerades rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen, samt dataombudsmannens kontaktuppgifter.

Den personuppgiftsansvarige ska ge den registrerade en beskrivning som avses i 1 mom. och annan behövlig information för utövande av den registrerades rättigheter enligt detta kapitel, om lämnande av denna information behövs i ett enskilt fall för att nämnda rättigheter ska kunna utövas. Den personuppgiftsansvarige får helt eller delvis låta bli att lämna informationen, om det är nödvändigt på de grunder som nämns i 28 §.

23 §

De registrerades rätt till insyn

Var och en har rätt att av den personuppgiftsansvarige få veta huruvida personuppgifter som gäller honom eller henne behandlas. Om sådana uppgifter behandlas, har den registrerade rätt att få följande information av den personuppgiftsansvarige:
1) vilka personuppgifter som behandlas och all tillgänglig information om varifrån uppgifterna kommer,
2) ändamålen med och den rättsliga grunden för behandlingen,
3) de kategorier av personuppgifter som behandlingen gäller,
4) de mottagare eller kategorier av mottagare till vilka den registrerades personuppgifter har lämnats ut,
5) den period under vilken personuppgifterna kommer att bevaras eller, om den inte har fastställts, kriterierna för att fastställa denna period,
6) uppgift om den registrerades rätt att av den personuppgiftsansvarige yrka att de personuppgifter som rör den registrerade rättas eller utplånas eller att behandlingen av dem begränsas,
7) uppgift om den registrerades rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen, samt dataombudsmannens kontaktuppgifter.

Den som önskar kontrollera uppgifter om sig själv på det sätt som avses i 1 mom., kan begära detta hos den personuppgiftsansvarige genom en egenhändigt undertecknad handling eller på ett därmed jämförbart bestyrkt sätt eller begära detta personligen hos den personuppgiftsansvarige.

24 §

Inskränkningar i rätten till insyn

Den registrerades rätt till insyn kan helt eller delvis skjutas upp, begränsas eller vägras till den del det är nödvändigt på de grunder som nämns i 28 §. Om den registrerades rätt till insyn skjuts upp, begränsas eller vägras, ska den personuppgiftsansvarige utan obefogat dröjsmål informera den registrerade om detta genom ett skriftligt intyg. Även grunderna för uppskovet, begränsningen eller vägran ska uppges, utom i det fall att lämnandet av denna information skulle äventyra syftet med vägran eller begränsningen. Om den personuppgiftsansvarige inte

inom tre månader efter att begäran framställts har gett den registrerade ett skriftligt svar, betraktas detta som att insyn har vägrats.

Den personuppgiftsansvarige ska informera den registrerade om dennes rätt att lämna in en begäran om åtgärder till dataombudsmannen på grund av att rätten till insyn skjutits upp, begränsats eller vägrats samt om dennes rätt att i enlighet med 29 § utöva rätten till insyn via dataombudsmannen.

Den personuppgiftsansvarige ska bevara information om de grunder på vilka rätten till insyn vägrats eller begränsats.

25 §

Rättelse eller utplåning av personuppgifter eller begränsning av behandlingen

Den personuppgiftsansvarige ska på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål rätta eller komplettera sådana personuppgifter om den registrerade som är oriktiga eller bristfälliga med hänsyn till ändamålet med behandlingen.

Den personuppgiftsansvarige ska på eget initiativ eller på yrkande av den registrerade utan obefogat dröjsmål utplåna personuppgifter om den registrerade, om behandlingen av dem står i strid med bestämmelserna i 4 eller 5 §, 6 § 1 eller 2 mom. eller 7 eller 11 §. I stället för utplåning ska den personuppgiftsansvarige dock begränsa behandlingen om

1) den registrerade bestrider personuppgifternas korrekthet och det inte kan fastställas huruvida de är korrekta, eller

2) personuppgifterna måste bevaras som bevisning.

Om behandlingen har begränsats med stöd av 2 mom. 1 punkten, ska den personuppgiftsansvarige innan begränsningen av behandlingen upphävs informera den registrerade om detta.

26 §

Vägran att godkänna den registrerades yrkande

Om inte den personuppgiftsansvarige godkänner den registrerades yrkande om rättelse, komplettering eller utplåning av personuppgifter eller begränsning av behandlingen av dem, ska den personuppgiftsansvarige genom ett skriftligt intyg informera den registrerade om vägran och grunderna för vägran. Den personuppgiftsansvarige får helt eller delvis låta bli att lämna den registrerade information om grunderna för vägran, om det är nödvändigt på de grunder som nämns i 28 §.

Den personuppgiftsansvarige ska informera den registrerade om att denne har rätt att lämna in en begäran om åtgärder till dataombudsmannen på grund av vägran enligt 1 mom. samt om att den registrerade har rätt att i enlighet med 29 § utöva de rättigheter som avses i 25 § via dataombudsmannen.

27 §

Den personuppgiftsansvariges skyldighet att informera om rättelse, utplåning eller begränsning av behandlingen

Den personuppgiftsansvarige ska anmäla varje rättelse av oriktiga personuppgifter till den myndighet från vilken de oriktiga personuppgifterna kommer.

Om personuppgifter har rättats eller utplånats eller behandlingen av dem har begränsats med stöd av 25 §, ska den personuppgiftsansvarige informera de mottagare om saken till vilka den personuppgiftsansvarige har lämnat ut uppgifterna. Mottagarna ska rätta eller utplåna de personuppgifter de har eller begränsa behandlingen av dem.

28 §

Begränsning av de registrerades rättigheter

De registrerades rättigheter får begränsas på det sätt som anges i 22 § 2 mom., 24 § 1 mom., 26 § 1 mom. och 35 §, om det med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd i syfte att

1) undvika menlig inverkan på förebyggande, avslöjande, utredning av brott eller på åtgärder som avser åtal för brott eller på verkställighet av straffrättsliga påföljder,

2) trygga andra undersökningar, utredningar eller motsvarande förfaranden hos myndigheter,

3) skydda den allmänna säkerheten,

4) skydda den nationella säkerheten, eller

5) skydda andra personers rättigheter.

29 §

Utövande av rättigheter via dataombudsmannen

Den registrerade har rätt att be dataombudsmannen kontrollera lagenligheten i personuppgifter och behandlingen av dem, om den registrerades rätt till insyn har skjutits upp, begränsats eller vägrats med stöd av denna eller någon annan lag eller om den personuppgiftsansvarige inte godkänner den registrerades yrkande om rättelse, komplettering eller utplåning av personuppgifterna eller begränsning av behandlingen av dem.

Om den registrerade utövar sin rätt enligt 1 mom., ska dataombudsmannen inom en rimlig tid informera den registrerade om vilka åtgärder dataombudsmannen har vidtagit. Dataombudsmannen ska också informera den registrerade om dennes rätt att lämna in en i 56 § avsedd begäran om åtgärder till dataombudsmannen.

30 §

Främjande av de registrerades möjligheter att utöva sina rättigheter samt avgiftsfria åtgärder

Den personuppgiftsansvarige ska främja de registrerades möjligheter att utöva de rättigheter som avses i detta kapitel. Alla meddelanden och all information om behandling av personuppgifter som lämnas till de registrerade ska tillhandahållas i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk.

Meddelanden och information som ska ges de registrerade enligt denna lag samt behandlingen av begäranden som de registrerade framställt i enlighet med denna lag är avgiftsfria för de registrerade. Om en registrerads begäranden på grund av att de upprepats eller av någon annan orsak är uppenbart orimliga eller ogrundade, får den personuppgiftsansvarige dock för åtgärden ta ut en avgift. Bestämmelser om grunderna för avgiftens belopp finns i lagen om grunderna för avgifter till staten (150/1992).

Om den personuppgiftsansvarige tar ut en avgift med stöd av 2 mom., ska den personuppgiftsansvarige vid behov visa att begäran har varit uppenbart ogrundad eller orimlig.

5 kap.

Informationssäkerhet

31 §

Skydd av personuppgifter

Den personuppgiftsansvarige och personuppgiftsbiträdet ska genom tekniska och organisatoriska åtgärder se till att personuppgifterna är tillräckligt skyddade med hänsyn till den risk för den registrerades rättigheter som behandlingen medför. Personuppgifterna ska särskilt skyddas för obehörig behandling och mot förlust, förstöring eller skada genom olyckshändelse. Åtgärderna ska planeras och genomföras med beaktande av

1) den senaste tekniska utvecklingen,
2) kostnaderna för att genomföra åtgärderna,
3) behandlingens art, omfattning, sammanhang och ändamål,
4) riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter.

32 §

Skydd av personuppgifter vid automatiserad behandling

Utöver vad som föreskrivs i 31 § ska den personuppgiftsansvarige eller personuppgiftsbiträdet när det gäller automatiserad databehandling, efter en bedömning av riskerna, vidta åtgärder i syfte att

1) vägra varje obehörig person åtkomst till den utrustning som används för behandling,
2) förhindra obehörig läsning, kopiering, ändring och utplåning av datamedier,
3) förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring och utplåning av lagrade personuppgifter,
4) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring,
5) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet,
6) säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring,
7) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes,
8) förhindra obehörig läsning, kopiering, ändring och utplåning av personuppgifter i samband med överföring av sådana uppgifter eller under transport av datamedier,
9) säkerställa att de system som används kan återställas vid störningar,
10) säkerställa att systemet fungerar, funktionsfel rapporteras och de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet.

33 §

Personuppgiftsbiträdets skyldighet att informera om en personuppgiftsincident

Personuppgiftsbiträdet ska efter att ha fått kännedom om en personuppgiftsincident utan obefogat dröjsmål informera den personuppgiftsansvarige om incidenten.

34 §

Den personuppgiftsansvariges skyldighet att anmäla en personuppgiftsincident till dataombudsmannen

Den personuppgiftsansvarige ska anmäla en personuppgiftsincident till dataombudsmannen, utom när det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för den registrerades rättigheter.

Den personuppgiftsansvarige ska göra anmälan enligt 1 mom. utan obefogat dröjsmål och om möjligt inom 72 timmar efter att ha fått kännedom om incidenten. Om anmälan till dataombudsmannen görs senare än så, ska skälen till fördröjningen nämnas i anmälan.

Den personuppgiftsansvarige ska bevara uppgifter om personuppgiftsincidenter och omständigheter i samband med dem, deras effekter och de korrigerande åtgärder som vidtagits.

35 §

Den personuppgiftsansvariges skyldighet att informera den registrerade om en personuppgiftsincident

Den personuppgiftsansvarige ska utan obefogat dröjsmål informera den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en betydande risk för den registrerades rättigheter. Informationsskyldighet föreligger dock inte, om

1) den personuppgiftsansvarige på de personuppgifter som påverkades av personuppgiftsincidenten har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder som effektivt förhindrar missbruk av uppgifterna, eller

2) den personuppgiftsansvarige efter incidenten har vidtagit åtgärder för att säkerställa att incidenten sannolikt inte kommer att medföra en risk för den registrerades rättigheter.

Den personuppgiftsansvarige kan i stället för att lämna information till den registrerade upplysa om personuppgiftsincidenten genom information till allmänheten, om det skulle kräva orimliga ansträngningar att informera de registrerade.

Informationen till den registrerade kan skjutas upp, begränsas eller utelämnas, om de förutsättningar som anges i 28 § uppfylls.

36 §

Den personuppgiftsansvariges skyldighet att informera andra personuppgiftsansvariga om en personuppgiftsincident

Den personuppgiftsansvarige ska utan obefogat dröjsmål lämna en anmälan om en personuppgiftsincident till personuppgiftsansvariga i Finland eller i andra EU-medlemsstater, om incidenten gäller personuppgifter som har överförts av eller till de personuppgiftsansvariga i fråga.

37 §

Innehållet i anmälan om en personuppgiftsincident

En anmälan enligt 34 § till dataombudsmannen och en anmälan enligt 36 § till personuppgiftsansvariga i Finland eller i andra EU-medlemsstater ska innehålla en beskrivning av personuppgiftsincidenten. Beskrivningen ska om möjligt inbegripa de kategorier av registrerade och det ungefärliga antal registrerade som berörs samt de kategorier av personuppgifter och det ungefärliga antal personuppgiftsposter som berörs.

Den information enligt 35 § som lämnas till den registrerade ska innehålla en beskrivning av personuppgiftsincidentens art.

Av de anmälningar och den information som avses i 1 och 2 mom. ska ytterligare framgå

1) namnet på och kontaktuppgifterna för dataskyddsombudet eller en annan kontaktpunkt där mer information kan erhållas,
2) de sannolika konsekvenserna av personuppgiftsincidenten,
3) de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten och vid behov åtgärder för att mildra dess negativa effekter.

Den information som lämnas till dataombudsmannen och till personuppgiftsansvariga i Finland eller i andra EU-medlemsstater får tillhandahållas i omgångar till den del det inte är möjligt att tillhandahålla informationen samtidigt.

6 kap.

Dataskyddsombud

38 §

Utnämning av dataskyddsombud

Den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Dataskyddsombudet ska ha tillräcklig sakkunskap om lagstiftning och praxis i fråga om behandling av personuppgifter samt förmåga att sköta de uppgifter som avses i 40 §. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter, om det är motiverat med hänsyn till myndigheternas organisationsstruktur och storlek.

Den personuppgiftsansvarige ska meddela dataombudsmannen dataskyddsombudets kontaktuppgifter.

39 §

Dataskyddsombudets ställning

Den personuppgiftsansvarige ska på ett korrekt sätt och i god tid se till att dataskyddsombudet deltar i alla frågor som rör skyddet av personuppgifter.

Den personuppgiftsansvarige ska ge dataskyddsombudet verksamhetsförutsättningar att sköta de uppgifter som denne ansvarar för enligt 40 § samt ge tillgång till personuppgifter och behandlingsförfaranden.

40 §

Dataskyddsombudets uppgifter

Dataskyddsombudet ska
1) ge råd i frågor som gäller skydd av personuppgifter till den personuppgiftsansvarige och den personal hos den personuppgiftsansvarige som behandlar personuppgifter,
2) övervaka att de bestämmelser som gäller behandling av personuppgifter och den personuppgiftsansvariges förfaranden för behandling av personuppgifter iakttas,
3) på begäran ge råd om konsekvensbedömningen avseende dataskydd och övervaka att den genomförs i enlighet med 20 §,
4) samarbeta med dataombudsmannen och vara kontaktpunkt för dataombudsmannen i frågor som gäller behandling av personuppgifter.

Dataskyddsombudets uppgifter omfattar inte rättskipningsverksamhet i domstolarna eller laglighetskontroll som utförs av justitiekanslern i statsrådet och riksdagens justitieombudsman.

7 kap.

Överföringar av personuppgifter till tredjeländer och internationella organisationer

41 §

Allmänna principer för överföring av personuppgifter

En behörig myndighet får överföra personuppgifter till ett tredjeland eller en internationell organisation endast om de övriga bestämmelser som är tillämpliga på behandling av personuppgifter enligt denna lag iakttas och

1) överföringen behövs för ett ändamål som nämns i 1 § 1 mom.,

2) personuppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är behörig att behandla personuppgifter för ett ändamål som nämns i 1 § 1 mom., och

3) det finns ett i artikel 36 i dataskyddsdirektivet avsett giltigt beslut av Europeiska kommissionen (kommissionen) om adekvat skyddsnivå eller, om inget sådant beslut har antagits, lämpliga skyddsåtgärder föreligger i enlighet med 42 § i denna lag eller undantag för särskilda situationer blir tillämpliga i enlighet med 43 §.

Om personuppgifterna har erhållits från en annan EU-medlemsstat, är en ytterligare förutsättning för överföring att medlemsstaten i fråga har gett tillstånd till överföringen. Överföringar som görs utan ett sådant tillstånd är tillåtna endast om överföringen är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en stat eller mot en EU-medlemsstats väsentliga intressen och tillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska informeras om överföringen utan dröjsmål.

Om personuppgifterna överförs vidare till ett annat tredjeland eller en annan internationell organisation, får den behöriga myndighet som gjorde den ursprungliga överföringen godkänna vidareöverföringen med iakttagande av bestämmelserna i 1 och 2 mom. och med vederbörligt beaktande av brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i det tredjeland till vilket eller den internationella organisation till vilken personuppgifterna förs vidare, samt andra relevanta omständigheter.

42 §

Överföring på basis av lämpliga skyddsåtgärder

Om kommissionen inte har antagit ett beslut som avses i 41 § 1 mom. 3 punkten, får personuppgifter överföras till ett tredjeland eller en internationell organisation, om de övriga förutsättningar som anges i 41 § uppfylls, och

1) lämpliga skyddsåtgärder för personuppgifter har fastställts i en rättsligt bindande handling, eller

2) den personuppgiftsansvarige efter att ha bedömt alla omständigheter kring en överföring av personuppgifter drar slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

Den personuppgiftsansvarige ska informera dataombudsmannen om de kategorier av överföringar som gjorts enligt 1 mom. 2 punkten. I fråga om överföringarna ska följande uppgifter bevaras och på begäran göras tillgängliga för dataombudsmannen:

1) datum och tidpunkt för överföringarna,

2) den mottagande behöriga myndigheten,

3) grunderna för överföringarna, och

4) de personuppgifter som har överförts.

43 §

Undantag i särskilda situationer

Om kommissionen inte har antagit ett beslut som avses i 41 § 1 mom. 3 punkten och de förutsättningar för uppgiftsöverföring som anges i 42 § inte uppfylls, får personuppgifter överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig

1) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,

2) för att skydda intressen som är berättigade och av stor betydelse för den registrerade,

3) för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en EU-medlemsstat eller ett tredjeland, eller

4) i enskilda fall för de ändamål som nämns i 1 § 1 mom. eller för att fastställa, göra gällande eller försvara rättsliga anspråk som hänför sig till dem.

Personuppgifter får dock inte överföras med stöd av 1 mom. 4 punkten, om den berörda registrerades rättigheter ska anses väga tyngre än det allmännas intresse av en sådan överföring.

I fråga om överföringar som baserar sig på 1 mom. ska följande uppgifter bevaras och på begäran göras tillgängliga för dataombudsmannen:

1) datum och tidpunkt för överföringen,

2) den mottagande behöriga myndigheten,

3) grunderna för överföringen, och

4) de personuppgifter som har överförts.

44 §

Överföring av personuppgifter till enskilda mottagare och andra mottagare i tredjeländer

Trots vad som föreskrivs i 41 § 1 mom. 2 punkten får en behörig myndighet i ett enskilt fall överföra personuppgifter direkt till enskilda mottagare och andra mottagare som är etablerade i tredjeländer, om de övriga bestämmelserna i denna lag iakttas och

1) överföringen är nödvändig för att en överförande behörig myndighet ska kunna utföra en uppgift enligt 1 § 1 mom. som den har ansvar för,

2) den behöriga myndighet som överför uppgifterna anser att den berörda registrerades rättigheter inte väger tyngre än det allmänna intresse som gör överföringen behövlig i det aktuella fallet,

3) den behöriga myndighet som överför uppgifterna, på grund av ärendets brådskande natur eller av någon annan orsak, anser att en överföring till en behörig myndighet i tredjelandet skulle vara ineffektiv eller olämplig,

4) den myndighet i tredjelandet som är behörig för de ändamål som avses i 1 § 1 mom. utan obefogat dröjsmål informeras om överföringen, om inte detta skulle vara ineffektivt eller olämpligt,

5) den behöriga myndighet som överför uppgifterna informerar mottagaren om det eller de specifika ändamål för vilket eller vilka personuppgifterna får behandlas, att behandlingen ska vara nödvändig för dessa ändamål och att uppgifterna inte får behandlas för andra ändamål, och

6) överföringen inte strider mot Finlands internationella avtalsförpliktelser.

Den behöriga myndighet som överför uppgifterna ska bevara information om varje överföring som utförs med stöd av 1 mom. och informera dataombudsmannen om överföringen.

8 kap.

Tillsynsmyndighet

45 §

Dataombudsmannen

Tillsyn över efterlevnaden av denna lag utövas av dataombudsmannen enligt 8 § i dataskyddslagen (/).

Bestämmelserna om tillsyn i denna lag tillämpas inte på domstolarna, justitiekanslern i statsrådet och riksdagens justitieombudsman

Dataombudsmannen är självständig och oberoende vid skötseln av sina uppgifter enligt denna lag.

46 §

Uppgifter

Dataombudsmannen ska, utöver att utöva tillsyn över efterlevnaden av denna lag

1) öka allmänhetens medvetenhet om risker, lagstiftning, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter,

2) öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om deras skyldigheter enligt denna lag,

3) på begäran tillhandahålla information till registrerade om hur de ska utöva de rättigheter de har enligt denna lag,

4) ge rådgivning vid förhandssamråd enligt 21 §,

5) göra utredningar om efterlevnaden av denna lag,

6) kontrollera lagenligheten i behandlingen i enlighet med 29 §,

7) behandla begäranden om åtgärder från registrerade eller från samfund som avses i 56 §,

8) följa sådan teknisk och annan utveckling som påverkar skyddet av personuppgifter.

Dataombudsmannen ska dessutom bidra till verksamheten i den dataskyddsstyrelse som avses i artikel 68 i 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 (allmän dataskyddsförordning). Dataombudsmannen ska dock inte föra sådana ärenden till dataskyddsstyrelsen som gäller behandling av personuppgifter i samband med verksamhet som avses i 1 § 2 mom.

Dataombudsmannens åtgärder är avgiftsfria för registrerade och för dataskyddsombud. Om en registrerads eller ett dataskyddsombuds begäranden dock på grund av att de upprepas eller av någon annan orsak är uppenbart orimliga eller ogrundade, kan dataombudsmannen ta ut avgift för åtgärderna eller lämna det ärende som begäran gäller utan prövning. Bestämmelser om grunderna för avgiftens belopp finns i lagen om grunderna för avgifter till staten.

Om dataombudsmannen på det sätt som avses i 3 mom. tar ut en avgift eller lämnar ärendet utan prövning, ska dataombudsmannen vid behov visa att begäran är uppenbart ogrundad eller orimlig.

47 §

Rätt att få information

Dataombudsmannen har trots sekretessbestämmelserna rätt att avgiftsfritt få en i 22 § avsedd beskrivning över behandlingsåtgärderna, de i 19 § avsedda logguppgifterna samt övriga uppgifter som behövs för att dataombudsmannen ska kunna sköta sina uppgifter.

Dataombudsmannen har rätt att av personuppgiftsansvariga och personuppgiftsbiträden få upplysningar om omständigheter som dataombudsmannen behöver för att kunna sköta sina uppgifter.

48 §

Rätt att utföra inspektioner

Dataombudsmannen får utföra inspektioner i en personuppgiftsansvarigs eller ett personuppgiftsbiträdes utrymmen, om en inspektion behövs för tillsynen över efterlevnaden av denna lag.

I utrymmen som används för boende av permanent natur får inspektion utföras endast om det är nödvändigt för att utreda de omständigheter som är föremål för inspektion och det i det aktuella fallet finns motiverade och specificerade skäl att misstänka att det har skett eller kommer att ske en sådan överträdelse av bestämmelserna om behandling av personuppgifter att påföljden kan vara ett straff enligt strafflagen (39/1889).

På inspektionerna tillämpas 39 § i förvaltningslagen (434/2003).

49 §

Handräckning

Dataombudsmannen har rätt att på begäran få handräckning av polisen för att utföra sina uppgifter.

50 §

Anlitande av sakkunniga

Dataombudsmannen får höra utomstående sakkunniga och begära utlåtanden från dem.

Dataombudsmannen får vid inspektioner som avses i 48 § anlita biträde av utomstående sakkunniga. Dataombudsmannen kan till sakkunnig utse en person som givit sitt samtycke till uppdraget och som innehar avsevärd sakkunskap med tanke på skötseln av dataombudsmannens uppgifter.

På en sakkunnig tillämpas bestämmelserna om straffrättsligt tjänsteansvar när han eller hon sköter uppgifter som avses i denna lag. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

51 §

Åtgärder

Dataombudsmannen kan i ärenden som omfattas av tillämpningsområdet för denna lag

1) ge den personuppgiftsansvarige handledning vid det förfarande för förhandssamråd som avses i 21 §,

2) informera den personuppgiftsansvarige eller personuppgiftsbiträdet om påstådda överträdelser av bestämmelserna i denna lag,

3) utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar kan stå i strid med denna lag,

4) ge den personuppgiftsansvarige eller personuppgiftsbiträdet en anmärkning, om denne behandlat personuppgifter i strid med lag,

5) ålägga den personuppgiftsansvarige eller personuppgiftsbiträdet att iaktta den registrerades begäranden om utövande av den registrerades rättigheter enligt denna lag,

6) ålägga den personuppgiftsansvarige att informera den registrerade om en personuppgiftsincident,

7) meddela ett tillfälligt eller bestående förbud eller ställa upp någon annan tillfällig eller bestående begränsning av behandlingen,
8) bestämma att överföring av uppgifter ska avbrytas till mottagare i tredjeländer eller internationella organisationer,
9) bestämma om rättelse och utplåning av personuppgifter och om begränsning av behandlingen samt andra åtgärder i samband med dem på basis av 25 §,
10) ålägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med bestämmelserna i denna lag, vid behov på ett bestämt sätt och inom en rimlig tid.

52 §

Vite

Dataombudsmannen får förena ett i 51 § 5—10 punkten avsett beslut samt ett sådant föreläggande att lämna ut uppgifter som grundar sig på 47 § med vite. Bestämmelser om föreläggande och utdömande av vite finns i viteslagen (1113/1990).
Ett i 1 mom. avsett föreläggande att lämna ut uppgifter får inte förenas med ett vitesföreläggande riktat till en fysisk person, om det finns anledning att misstänka personen för brott och uppgifterna gäller en omständighet som har samband med brottsmisstanken.

53 §

Hörande av dataombudsmannen

Dataombudsmannen kan på eget initiativ eller på begäran yttra sig i frågor som hänför sig till sådan behandling av personuppgifter som avses i 1 §.
Dataombudsmannen ska ges tillfälle att bli hörd vid beredningen av lagstiftnings- eller förvaltningsreformer som gäller sådan behandling av personuppgifter som avses i 1 §.

54 §

Ömsesidigt bistånd

Dataombudsmannen ska trots sekretessbestämmelserna avgiftsfritt ge motsvarande tillsynsmyndighet i en annan EU-medlemsstat de personuppgifter som myndigheten nödvändigt behöver i sitt tillsynsuppdrag samt andra behövliga uppgifter, och vid behov även annars bistå myndigheten vid utövandet av tillsynen. Dataombudsmannen ska vidta också andra behövliga åtgärder för att säkerställa ett effektivt samarbete.
Dataombudsmannen ska besvara en begäran från en tillsynsmyndighet som avses i 1 mom. utan obefogat dröjsmål och inte senare än en månad efter det att dataombudsmannen tagit emot begäran.

9 kap.

Rättsskydd

55 §

Rapportering av överträdelser

Den behöriga myndigheten ska ha förfaranden som gör det möjligt att konfidentiellt till myndigheten rapportera en misstänkt överträdelse av bestämmelserna i denna lag. Rapporteringsförfarandet ska omfatta lämpliga och tillräckliga åtgärder för att ordna en korrekt behandling av rapporterna. Rapporteringsförfarandet ska dessutom omfatta anvisningar som tryggar skyddet för rapportörens identitet.

Den behöriga myndigheten ska bevara behövlig information om sådana rapporter som avses i 1 mom. Informationen ska avföras fem år efter rapporteringen, om inte informationen fortsättningsvis behövs för en brottsutredning, en pågående rättegång eller en myndighetsundersökning eller för att trygga de rättigheter som rapportören eller den som är föremål för rapporten har. Senast tre år efter den föregående kontrollen ska behovet av fortsatt bevarande undersökas. En anteckning ska göras om kontrollen.

När en fysisk person till den behöriga myndigheten har lämnat en rapport som avses i 1 mom., ska rapportörens identitet hållas hemlig, om det utifrån omständigheterna kan bedömas vara till nackdel för rapportören att hans eller hennes identitet röjs.

56 §

Rätt att föra ärenden till dataombudsmannen

En registrerad har rätt att föra ett ärende till dataombudsmannen för behandling (*begäran om åtgärder*), om den registrerade anser att någon vid behandlingen av hans eller hennes personuppgifter bryter mot denna lag eller någon annan lag som gäller behandling av personuppgifter. Med den registrerades samtycke får ärendet föras till dataombudsmannen också av ett allmännyttigt samfund som främjar skyddet av personuppgifter.

57 §

Behandlingen av en begäran om åtgärder

Dataombudsmannen prövar det ärende som avses i begäran om åtgärder, om inte ärendet är anhängigt i domstol. Dataombudsmannen ska inom rimlig tid informera den som inlett ärendet om hur behandlingen fortskrider, om behandlingen av ärendet fördröjs på grund av att en ytterligare utredning behövs eller av något annat skäl.

Om dataombudsmannen i ett ärende som inletts hos dataombudsmannen anser att det behöver utredas om ett i 41 § 1 mom. 3 punkten avsett beslut av kommissionen om adekvat skyddsnivå är förenligt med dataskyddsdirektivet, får dataombudsmannen genom en ansökan föra ärendet till Helsingfors förvaltningsdomstol för avgörande.

58 §

Ändringssökande

Dataombudsmannens beslut får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd. Även dataombudsmannen får söka ändring i förvaltningsdomstolens beslut.

I dataombudsmannens beslut får det bestämmas att beslutet ska iakttas trots ändringssökande, om inte besvärsmyndigheten bestämmer något annat.

10 kap.

Särskilda bestämmelser

59 §

Skadestånd

Den personuppgiftsansvarige är skyldig att ersätta den registrerade eller någon annan person för ekonomisk skada och annan skada som denne har tillfogats av att personuppgifter har behandlats i strid med denna lag.

Bestämmelser i övrigt om rätten till skadestånd finns i skadeståndslagen.

60 §

Straffbestämmelser

Bestämmelser om straff för dataskyddsbrott finns i 38 kap. 9 § i strafflagen. Bestämmelser om straff för kränkning av kommunikationshemlighet finns i 3 § och för grov kränkning av kommunikationshemlighet i 4 § det kapitlet samt bestämmelser om straff för dataintrång i 8 § och för grovt dataintrång i 8 a § i det kapitlet. Till straff för brott mot tystnadsplikten enligt i 61 § i denna lag döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte gärningen utgör brott enligt 40 kap. 5 § i den lagen eller om inte strängare straff för den föreskrivs någon annanstans i lag.

61 §

Tystnadsplikt

Den som har deltagit i behandlingen av personuppgifter får inte obehörigen för utomstående röja de uppgifter som han eller hon erhållit på detta sätt eller använda uppgifterna för sin egen eller någon annans vinning eller för att skada någon annan.

11 kap.

Ikraftträdande och övergångsbestämmelser

62 §

Ikraftträdande

Denna lag träder i kraft den 20 .

63 §

Övergångsbestämmelser

Automatiserade behandlingssystem som har inrättats före den 6 maj 2016 ska bringas i överensstämmelse med 19 § senast den 6 maj 2023.

_____

2.

Lag

om ändring av 1 och 6 § i straffregisterlagen

I enlighet med riksdagens beslut

ändras i straffregisterlagen (770/1993) 1 § 1 mom. och 6 § 8 mom., sådana de lyder, 1 § 1 mom. i lag 1093/1999 och 6 § 8 mom. i lag 215/2012, som följer:

1 §

Personuppgiftsansvarig i fråga om straffregistret är Rättsregistercentralen.

— —

6 §

— —

Den som har rätt att teckna en juridisk persons namn har rätt att på begäran få ett i 5 § 1 mom. avsett straffregisterutdrag som gäller den juridiska personen.

———

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen

I enlighet med riksdagens beslut

ändras i lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012) 4 § 3 mom. samt 8 och 13 § som följer:

4 §

Förhållande till andra lagar och internationella förpliktelser

— —

Om inte något annat föreskrivs i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999) på sekretess för samt utlämnande och skydd av personuppgifter samt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) på annan behandling av personuppgifter.

8 §

Lagringsregistrets syfte

Personuppgiftsansvarig i fråga om lagringsregistret är Rättsregistercentralen. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.

13 §

Rätt till insyn

I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt.

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av lagen om justitieförvaltningens riksomfattande informationssystem

I enlighet med riksdagens beslut

upphävs i lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) 18 § 2 mom., och

ändras 2 § 1 mom., den svenska språkdräkten i 7 § 1 mom. och i 7 § 3 mom. 3 punkten samt 10 § 2 mom. och 19 § som följer:

2 §

Förhållande till annan lagstiftning

Utöver vad som föreskrivs i denna lag finns det bestämmelser om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informationssystem och om de i systemet införda uppgifternas offentlighet i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt bestämmelser om behandling av personuppgifter i 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 (allmän dataskyddsförordning), nedan dataskyddsförordningen, i dataskyddslagen (/) och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

— —

7 §

Åtaganden i samband med förvaltningen och utvecklingen av informationssystemet

Rättsregistercentralen är personuppgiftsansvarig i fråga om justitieförvaltningens riksomfattande informationssystem.

— —

De myndigheter som fört in uppgifter i justitieförvaltningens riksomfattande informationssystem är skyldiga att se till att

— —

3) anteckningarna har gjorts i enlighet med de tekniska krav som den personuppgiftsansvarige ställt

10 §

Personuppgifter som ska registreras i informationssystemet

— —

I registret över avgöranden och meddelanden om avgöranden får det i fråga om fysiska personer som har del i saken endast antecknas sådana i artikel 9 i dataskyddsförordningen och i 11 § i lagen om behandling av personuppgifter i brottmål eller vid upprätthållandet av den nationella säkerheten avsedda personuppgifter som tillhör särskilda kategorier av personuppgifter och som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av

en justitieförvaltningsmyndighets avgörande och behövs för verkställighet av en dom, för registrering i myndighetsregister eller för fullgörande av andra uppgifter som enligt lag ska skötas av justitieförvaltningsmyndigheter..

19 §

Rätt till insyn och rättelse av uppgifter

I fråga om den registrerades rätt till insyn och rätt att få sina uppgifter rättade eller kompletterade föreskrivs särskilt.

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av lagen om verkställighet av böter

I enlighet med riksdagens beslut
upphävs i lagen om verkställighet av böter (672/2002) 49 §, och
ändras 46 och 48 § samt den svenska språkdräkten i 50 § 1 mom. som följer:

46 §

Ändamålet med bötesregistret och behandlingen av registeruppgifterna

Rättsregistercentralen (den personuppgiftsansvarige) förvaltar ett bötesregister som förs och används för verkställighet av ärenden som ska verkställas på det sätt som föreskrivs i denna lag.

Rätt att behandla uppgifter i bötesregistret har Rättsregistercentralens tjänstemän till den del det behövs för skötseln av tjänsteåliggandena.

Utöver vad som föreskrivs i denna lag eller i någon annan lag finns det bestämmelser om rätten att ta del av myndigheternas offentliga handlingar, om tystnadsplikt för myndigheter och om handlingssekretess, samt om andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att få uppgifter, i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt bestämmelser om annan behandling av personuppgifter i 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 (allmän dataskyddsförordning), i dataskyddslagen (/) och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).

48 §

Den personuppgiftsansvariges rätt att få uppgifter

Den personuppgiftsansvarige har för förvaltningen av bötesregistret och skötseln av lagenliga verkställighetsuppdrag rätt att ur befolkningsdatasystemet få uppgifter som gäller en fysisk persons namn, personbeteckning, adress och död samt andra motsvarande uppgifter som behövs för verkställigheten och har samband med att personen i fråga ska kunna påträffas, samt motsvarande uppgifter om juridiska personer av de behöriga registermyndigheterna.

50 §

Hemlighållande och utlämnande av uppgifter som ingår i bötesregistret

Uppgifterna i bötesregistret om brott och straffrättsliga påföljder ska hållas hemliga. Vid behandlingen av nämnda uppgifter ska den personuppgiftsansvarige iaktta särskild omsorg samt säkerställa en tillräcklig teknisk och organisatorisk skyddsnivå för registret.

———————————————————————————————————————

_____

Denna lag träder i kraft den 20 .

_____

6.

Lag

om ändring av lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten (1069/2015) 1 § 1 mom., den svenska språkdräkten i 11 §, i 24 § 2 mom. och i 28 § 3 mom., 30 och 31 §, den svenska språkdräkten i 32 §, 33 § 1 mom., den svenska språkdräkten i 34 § 3 mom. samt 37 § 2 mom., av dem 31 § sådan den lyder delvis ändrad i lag 17/2016, som följer:

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999) och på annan behandling av personuppgifter 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 (allmän dataskyddsförordning), nedan dataskyddsförordningen, samt dataskyddslagen (/) och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).
— —

11 §

Ansvar för uppgifternas riktighet

Den personuppgiftsansvarige och den enhet vid Brottspåföljdsmyndigheten som har fört in en uppgift i registret svarar för att den registrerade uppgiften är riktig.

24 §

Förfarandet för utlämnande av uppgifter i fall som avses i 14—23 §

— —
Beslut om utlämnande av uppgifter enligt 14—23 § fattas av den personuppgiftsansvarige eller en av denne utsedd tjänsteman vid Brottspåföljdsmyndigheten.

28 §

Rätt att få uppgifter av andra myndigheter och uppgiftsskyldiga

— —

De uppgifter som avses i 1 och 2 mom. kan lämnas genom teknisk anslutning så som särskilt avtalas med den personuppgiftsansvarige.

30 §

Information om behandling av uppgifter

Den personuppgiftsansvarige ska i enlighet med vad som föreskrivs i dataskyddsförordningen och dataskyddslagen informera den registrerade om behandling av uppgifter. Undantag från informationsplikten får dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.

31 §

Inskränkningar i rätten till insyn

Utöver vad som föreskrivs i dataskyddsförordningen, dataskyddslagen eller lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten får den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten eller mot säkerheten för en anställd vid Brottspåföljdsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret.

32 §

Utövande av rätten till insyn

Den registrerade ska personligen kontrollera sina uppgifter vid den enhet vid Brottspåföljdsmyndigheten som den personuppgiftsansvarige anvisar. När begäran om insyn framställs ska den registrerade styrka sin identitet. Den ovan avsedda enheten vid Brottspåföljdsmyndigheten ger den registrerade tillfälle att så som den personuppgiftsansvarige bestämmer kontrollera de uppgifter som han eller hon har rätt till insyn i.

33 §

Bevaring av uppgifter som konstaterats vara oriktiga

Oberoende av vad som i dataskyddsförordningen, dataskyddslagen eller lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottspåföljdsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.

— —

34 §

Granskning av uppgifter och gallring av uppgifter ur register

— —

Den personuppgiftsansvarige eller den enhet vid Brottspåföljdsmyndigheten som den personuppgiftsansvarige bestämt ska en gång per år granska om det finns behov av att bevara de uppgifter som lagrats och som ingår i säkerhetsregistret. Behovet av att bevara uppgifterna i besökarregistret ska granskas vartannat år. Behovet av att bevara uppgifterna i verkställighetsregistret, samhällspåföljdsregistret samt övervaknings- och verksamhetsregistret ska granskas vart tredje år.

— —

37 §

Straffbestämmelser

— —

Bestämmelser om straff för dataskyddsbrott finns i 38 kap. 9 § i strafflagen och bestämmelser om straff för dataintrång i 8 § och grovt dataintrång i 8 a § i det kapitlet.

_____

Denna lag träder i kraft den 20 .

_____

Helsingfors den 5 april 2018

Statsminister

Juha Sipilä

Justitieminister Antti Häkkänen

Bilaga
Parallelltext

2.

Lag

om ändring av 1 och 6 § i straffregisterlagen

I enlighet med riksdagens beslut
ändras i straffregisterlagen (770/1993) 1 § 1 mom. och 6 § 8 mom., sådana de lyder, 1 § 1 mom. i lag 1093/1999 och 6 § 8 mom. i lag 215/2012, som följer:

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
Vid rättsregistercentralen förs straffregister enligt vad som bestäms i denna lag	*Personuppgiftsansvarig i fråga om straffregistret är Rättsregistercentralen.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
6 §	6 §
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt. Den som antecknats i straffregistret har dessutom rätt att på begäran få veta till vem och för vilket ändamål det under det senaste året har lämnats ut uppgifter om honom eller henne ur ett sådant register som förs med hjälp av automatisk databehandling. Den som har rätt att teckna en juridisk persons namn har, *oberoende av det sätt på vilket registret förs*, motsvarande kontrollrätt och rätt att få information för den juridiska personens räkning samt rätt att få ett straffregisterutdrag som gäller den juridiska personen.	Den som har rätt att teckna en juridisk persons namn har rätt att *på begäran få* ett *i 5 § 1 mom. avsett* straffregisterutdrag som gäller den juridiska personen.

———

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen

I enlighet med riksdagens beslut

ändras i lagen om lagring av straffregisteruppgifter och om utlämnande av sådana uppgifter mellan Finland och de övriga medlemsstaterna i Europeiska unionen (214/2012) 4 § 3 mom. samt 8 och 13 § som följer:

Gällande lydelse	*Föreslagen lydelse*
4 §	4 §
Förhållande till andra lagar och internationella förpliktelser	*Förhållande till andra lagar och internationella förpliktelser*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Om inte något annat bestäms i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999) på sekretess för samt utlämnande och skydd av personuppgifter samt personuppgiftslagen (523/1999) på annan behandling av personuppgifter.	Om inte något annat föreskrivs i denna lag eller i någon annan lag tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999) på sekretess för samt utlämnande och skydd av personuppgifter *samt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/) på annan behandling av personuppgifter.*
8 §	8 §
Lagringsregistrets syfte	*Lagringsregistrets syfte*
Rättsregistercentralen ska föra ett lagringsregister. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.	*Personuppgiftsansvarig i fråga om lagringsregistret är Rättsregistercentralen*. Lagringsregistret förs i syfte att lagra uppgifter så att de kan vidarebefordras till andra medlemsstater och finska myndigheter samt antecknas i straffregisterutdrag enligt vad som föreskrivs i denna lag.
13 §	13 §
Kontrollrätt	***Rätt till insyn***
I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt. *Den som antecknats i lagringsregistret har dessutom rätt att på begäran få veta till vem och för vilket ändamål det under det senaste året har lämnats ut uppgifter om honom eller henne ur ett sådant register som förs med hjälp av automatisk databe-*	I fråga om vars och ens rätt att kontrollera sina egna registeruppgifter föreskrivs särskilt.

Gällande lydelse	*Föreslagen lydelse*
handling.	
	_____
	Denna lag träder i kraft den 20 .
	_____

4.

Lag

om ändring av lagen om justitieförvaltningens riksomfattande informationssystem

I enlighet med riksdagens beslut

upphävs i lagen om justitieförvaltningens riksomfattande informationssystem (372/2010) 18 § 2 mom., och

ändras 2 § 1 mom., den svenska språkdräkten i 7 § 1 mom. och i 7 § 3 mom. 3 punkten samt 10 § 2 mom. och 19 § som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Förhållande till annan lagstiftning	*Förhållande till annan lagstiftning*
Om inte något annat föreskrivs i denna lag, gäller i fråga om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informationssystem och i fråga om de i systemet införda uppgifternas offentlighet vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) samt i fråga om annan behandling av personuppgifter som förts in i systemet vad som föreskrivs i personuppgiftslagen (523/1999).	*Utöver vad som föreskrivs* i denna lag finns det bestämmelser om utlämnande av uppgifter ur justitieförvaltningens riksomfattande informationssystem och om de i systemet införda uppgifternas offentlighet i lagen om offentlighet i myndigheternas verksamhet (621/1999) *samt bestämmelser om behandling av personuppgifter i 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 (allmän dataskyddsförordning), nedan dataskyddsförordningen, i dataskyddslagen (/) och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
7 §	7 §
Åtaganden i samband med förvaltningen och utvecklingen av informationssystemet	*Åtaganden i samband med förvaltningen och utvecklingen av informationssystemet*
Rättsregistercentralen är registeransvarig för justitieförvaltningens riksomfattande informationssystem.	Rättsregistercentralen är *personuppgiftsansvarig* i fråga om justitieförvaltningens riksomfattande informationssystem.
De myndigheter som fört in uppgifter i justitieförvaltningens riksomfattande informationssystem är skyldiga att se till att	De myndigheter som fört in uppgifter i justitieförvaltningens riksomfattande informationssystem är skyldiga att se till att
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
3) anteckningarna har gjorts i enlighet med de tekniska krav som den registeran-	3) anteckningarna har gjorts i enlighet med de tekniska krav som den *personupp-*

Gällande lydelse	*Föreslagen lydelse*
svarige ställt.	*giftsansvarige* ställt.
10 §	10 §
Personuppgifter som ska registreras i informationssystemet	*Personuppgifter som ska registreras i informationssystemet*
I registret över avgöranden och meddelanden om avgöranden får det om fysiska personer i partsställning antecknas endast sådana enligt 11 § i personuppgiftslagen känsliga uppgifter som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av en justitieförvaltningsmyndighets avgörande och behövs för verkställighet av en dom, för registrering i myndighetsregister eller för fullgörande av andra justitieförvaltningsmyndigheters lagstadgade uppgifter.	I registret över avgöranden och meddelanden om avgöranden får det i fråga om fysiska personer *som har del i saken* endast antecknas sådana *i artikel 9 i dataskyddsförordningen och i 11 § i lagen om behandling av personuppgifter i brottmål eller vid upprätthållandet av den nationella säkerheten avsedda personuppgifter* som tillhör särskilda kategorier av personuppgifter och som ska registreras i domstolars diarie- eller andra dokumentregister eller som framgår av en justitieförvaltningsmyndighets avgörande och behövs för verkställighet av en dom, för registrering i myndighetsregister eller för fullgörande av andra *uppgifter som enligt lag ska skötas* av justitieförvaltningsmyndigheter.
19 §	19 §
Rätt till insyn och rättelse av uppgifter	*Rätt till insyn och rättelse av uppgifter*
En justitieförvaltningsmyndighet behandlar och avgör en registrerades begäran om rätt till insyn och korrigering av uppgifter endast om ärendet har behandlats och avgjorts av myndigheten i fråga och denna myndighet registrerat uppgifterna om ärendet i justitieförvaltningens riksomfattande informationssystem. *Rättsregistercentralen kan överföra en registrerads begäran om rätt till insyn eller rättelse av sina personuppgifter till den justitieförvaltningsmyndighet som har fört in uppgifterna om den registrerade i registret över avgöranden och meddelanden om avgöranden eller i rikssystemet för behandling av diarie- och ärendehanteringsuppgifter.* *Utan hinder av vad som i 27 § i personuppgiftslagen föreskrivs om rätten till insyn i register som används för statistik och vetenskaplig forskning har den registrerade rätt till insyn, om Rättsregistercentralen med stöd av 13 § i denna lag har använt uppgifter som överförts till rapporterings-,*	*I fråga om den registrerades rätt till insyn och rätt att få sina uppgifter rättade eller kompletterade föreskrivs särskilt.*

Gällande lydelse	*Föreslagen lydelse*
statistik- och arkivsystemet vid behandling av ärenden som berör den registrerade. *I fråga om registrerades rätt till insyn tillämpas i övrigt vad som föreskrivs i personuppgiftslagen.*	

_____

Denna lag träder i kraft den 20 .

_____

5.

Lag

om ändring av lagen om verkställighet av böter

I enlighet med riksdagens beslut
upphävs i lagen om verkställighet av böter (672/2002) 49 §, och
ändras 46 och 48 § samt den svenska språkdräkten i 50 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
46 §	46 §
Ändamålet med bötesregistret och behandlingen av registeruppgifterna	*Ändamålet med bötesregistret och behandlingen av registeruppgifterna*
Rättsregistercentralen (*registeransvarig*) upprätthåller ett bötesregister som förs och används för verkställighet av ärenden som skall verkställas i den ordning som föreskrivs i denna lag.	Rättsregistercentralen (***den personuppgiftsansvarige***) *förvaltar* ett bötesregister som förs och används för verkställighet av ärenden som ska verkställas på det sätt som föreskrivs i denna lag.
Rätt att behandla uppgifter i bötesregistret har Rättsregistercentralens tjänstemän till den del det behövs för skötseln av tjänsteåliggandena.	Rätt att behandla uppgifter i bötesregistret har Rättsregistercentralens tjänstemän till den del det behövs för skötseln av tjänsteåliggandena.
På behandlingen av uppgifter i bötesregistret tillämpas personuppgiftslagen (523/1999) och i fråga om utlämnande av uppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999), om inte något annat bestäms nedan.	*Utöver vad som föreskrivs i denna lag eller i någon annan lag finns det bestämmelser om rätten att ta del av myndigheternas offentliga handlingar, om tystnadsplikt för myndigheter och om handlingssekretess, samt om andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att få uppgifter,* i lagen om offentlighet i myndigheternas verksamhet (621/1999) *samt bestämmelser om annan behandling av personuppgifter i 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 (allmän dataskyddsförordning), i dataskyddslagen (/)* och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).
48 §	48 §

Gällande lydelse	*Föreslagen lydelse*
Den personuppgiftsansvariges rätt att få uppgifter	*Den personuppgiftsansvariges rätt att få uppgifter*
Den registeransvarige har för upprätthållandet av bötesregistret och skötseln av lagenliga verkställighetsuppdrag rätt att ur det centrala befolkningsregistret få uppgifter som gäller en fysisk persons namn, personbeteckning, adress och död samt andra motsvarande uppgifter som behövs för verkställigheten och har samband med att personen i fråga skall kunna påträffas samt motsvarande uppgifter om juridiska personer av de behöriga registermyndigheterna.	Den personuppgiftsansvarige har för *förvaltningen* av bötesregistret och skötseln av lagenliga verkställighetsuppdrag rätt att ur *befolkningsdatasystemet* få uppgifter som gäller en fysisk persons namn, personbeteckning, adress och död samt andra motsvarande uppgifter som behövs för verkställigheten och har samband med att personen i fråga ska kunna påträffas, samt motsvarande uppgifter om juridiska personer av de behöriga registermyndigheterna.
50 §	50 §
Hemlighållande och utlämnande av uppgifter som ingår i bötesregistret	*Hemlighållande och utlämnande av uppgifter som ingår i bötesregistret*
Uppgifterna i bötesregistret om brott och straffrättsliga påföljder skall hållas hemliga. Vid behandlingen av nämnda uppgifter skall den registeransvarige iaktta särskild omsorg samt säkerställa en tillräcklig teknisk och organisatorisk skyddsnivå för registret.	Uppgifterna i bötesregistret om brott och straffrättsliga påföljder ska hållas hemliga. Vid behandlingen av nämnda uppgifter ska den *personuppgiftsansvarige* iaktta särskild omsorg samt säkerställa en tillräcklig teknisk och organisatorisk skyddsnivå för registret.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

6.

Lag

om ändring av lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter vid Brottspåföljdsmyndigheten (1069/2015) 1 § 1 mom., den svenska språkdräkten i 11 §, i 24 § 2 mom. och i 28 § 3 mom., 30 och 31 §, den svenska språkdräkten i 32 §, 33 § 1 mom., den svenska språkdräkten i 34 § 3 mom. samt 37 § 2 mom., av dem 31 § sådan den lyder delvis ändrad i lag 17/2016, som följer:

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
Lagens tillämpningsområde	*Lagens tillämpningsområde*
Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999) och på annan behandling av personuppgifter personuppgiftslagen (523/1999).	Denna lag innehåller bestämmelser om förande av sådana personregister som behövs för skötseln av verkställighet av straff och andra uppdrag som hör till Brottspåföljdsmyndigheten samt om annan behandling av personuppgifter. Om inte något annat föreskrivs i denna lag, tillämpas på sekretess för och utlämnande av personuppgifter lagen om offentlighet i myndigheternas verksamhet (621/1999) och på annan behandling av personuppgifter *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 (allmän dataskyddsförordning), nedan dataskyddsförordningen, samt dataskyddslagen (/) och lagen om be-handling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (/).*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
11 §	11 §
Ansvar för uppgifternas riktighet	*Ansvar för uppgifternas riktighet*
Den registeransvarige och den enhet vid Brottspåföljdsmyndigheten som har fört in en uppgift i registret svarar för att den registrerade uppgiften är riktig.	Den *personuppgiftsansvarige* och den enhet vid Brottspåföljdsmyndigheten som har fört in en upp-gift i registret svarar för att den registrerade uppgiften är riktig.
24 §	24 §
Förfarandet för utlämnande av uppgifter i	*Förfarandet för utlämnande av uppgifter i*

Gällande lydelse	*Föreslagen lydelse*
fall som avses i 14—23 §	*fall som avses i 14—23 §*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Beslut om utlämnande av uppgifter enligt 14—23 § fattas av den registeransvarige eller en av denne utsedd tjänsteman vid Brottspåföljdsmyndigheten.	Beslut om utlämnande av uppgifter enligt 14—23 § fattas av den *personuppgiftsansvarige* eller en av denne utsedd tjänsteman vid Brottspåföljdsmyndigheten.
28 §	28 §
Rätt att få uppgifter av andra myndigheter och uppgiftsskyldiga	*Rätt att få uppgifter av andra myndigheter och uppgiftsskyldiga*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
De uppgifter som avses i 1 och 2 mom. kan lämnas genom teknisk anslutning så som särskilt avtalas med den registeransvarige.	De uppgifter som avses i 1 och 2 mom. kan lämnas genom teknisk anslutning så som särskilt avtalas med den *personuppgiftsansvarige.*
30 §	30 §
Information om behandling av uppgifter	*Information om behandling av uppgifter*
Den registeransvarige ska i enlighet med vad som föreskrivs i personuppgiftslagen informera den registrerade om behandling av uppgifter. Undantag från informationsplikten kan dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.	Den personuppgiftsansvarige ska i enlighet med vad som föreskrivs i *dataskyddsförordningen och dataskyddslagen* informera den registrerade om behandling av uppgifter. Undantag från informationsplikten får dock göras om det är nödvändigt för ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten.
31 §	31 §
Inskränkningar i rätten till insyn	*Inskränkningar i rätten till insyn*
Utöver vad som föreskrivs i personuppgiftslagen kan den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten eller mot säkerheten för en anställd vid Brottspåföljdsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret. (8.1.2016/17) *Dataombudsmannen kan på begäran av den registrerade kontrollera att de uppgifter*	Utöver vad som föreskrivs i dataskyddsförordningen, *dataskyddslagen eller lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten får* den registrerades rätt till insyn begränsas, om utövande av rätten till insyn på sannolika grunder kan leda till ett allvarligt hot mot ordningen och säkerheten i en enhet vid Brottspåföljdsmyndigheten eller mot säkerheten för en anställd vid Brottspåföljdsmyndigheten eller för någon annan. Den registrerade har inte rätt till insyn i uppgifter i säkerhetsregistret eller i de uppgifter om målsägande enligt 7 § 1 mom. 10 punkten i denna lag som ingår i övervaknings- och verksamhetsregistret.

Gällande lydelse	*Föreslagen lydelse*
om den registrerade som avses i 1 mom. är lagenliga.	
32 §	32 §
Utövande av rätten till insyn	*Utövande av rätten till insyn*
Den registrerade ska personligen kontrollera sina uppgifter vid den enhet vid Brottspåföljdsmyndigheten som den registeransvarige anvisar. När begäran om insyn framställs ska den registrerade styrka sin identitet. Den ovan avsedda enheten vid Brottspåföljdsmyndigheten ger den registrerade tillfälle att så som den registeransvarige bestämmer kontrollera de uppgifter som han eller hon har rätt till insyn i.	Den registrerade ska personligen kontrollera sina uppgifter vid den enhet vid Brottspåföljdsmyndigheten som den *personuppgiftsansvarige* anvisar. När begäran om insyn framställs ska den registrerade styrka sin identitet. Den ovan avsedda enheten vid Brottspåföljdsmyndigheten ger den registrerade tillfälle att så som den *personuppgiftsansvarige* bestämmer kontrollera de uppgifter som han eller hon har rätt till insyn i.
33 §	33 §
Bevaring av uppgifter som konstaterats vara oriktiga	*Bevaring av uppgifter som konstaterats vara oriktiga*
Oberoende av vad som i personuppgiftslagens föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottspåföljdsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.	Oberoende av vad som i *dataskyddsförordningen, dataskyddslagen eller lagen om behandling av personuppgifter i brottmål och vid upprätthållandet* av den nationella säkerheten föreskrivs om rättelse av oriktiga uppgifter i ett register får en oriktig uppgift bevaras i samband med den rättade uppgiften, om det behövs för att trygga rättigheterna för den registrerade, någon annan part eller en anställd vid Brottspåföljdsmyndigheten. En sådan uppgift får användas endast i det syfte som här avses.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
34 §	34 §
Granskning av uppgifter och gallring av uppgifter ur register	*Granskning av uppgifter och gallring av uppgifter ur register*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Den registeransvarige eller den enhet vid Brottspåföljdsmyndigheten som den registeransvarige bestämt ska en gång per år granska om det finns behov av att bevara de uppgifter som lagrats och som ingår i säkerhetsregistret. Behovet av att bevara uppgifterna i besökarregistret ska granskas vartannat år. Behovet av att bevara uppgifterna i verkställighetsregistret, samhällspåföljdsre-	Den *personuppgiftsansvarige* eller den enhet vid Brottspåföljdsmyndigheten som den personupp-giftsansvarige bestämt ska en gång per år granska om det finns behov av att bevara de uppgifter som lagrats och som ingår i säkerhetsregistret. Behovet av att bevara uppgifterna i besökarregistret ska granskas vartannat år. Behovet av att bevara uppgifterna i verkställighetsregistret, sam-

Gällande lydelse	*Föreslagen lydelse*
gistret samt övervaknings- och verksamhetsregistret ska granskas vart tredje år.	hällspåföljdsregistret samt övervakningsoch verksamhetsregistret ska granskas vart tredje år.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
37 §	37 §
Straffbestämmelser	*Straffbestämmelser*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Till straff för personregisterbrott döms enligt 38 kap. 9 § i strafflagen och till straff för dataintrång i personregister enligt 38 kap. 8 § i strafflagen. *Till straff för personregisterförseelse döms enligt 48 § 2 mom. i personuppgiftslagen.*	*Bestämmelser om straff för dataskyddsbrott finns i* 38 kap. 9 § i strafflagen och *bestämmelser om straff för dataintrång i 8 § och grovt dataintrång i 8 a § i det kapitlet.*
	————
	Denna lag träder i kraft den 20 .
	————