FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 10 december 2018

1054/2018

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 kap. 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 ovan 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.

RP 31/2018
FvUB 14/2018
RSv 113/2018

Europaparlamentets och rådets direktiv 2016/680/EU (32016L0680); EUT L 119, 4.5.2016, s. 89

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 uppgifts-

behandlingstjänster 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 riskerna 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 har 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 (1050/2018).

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 fängelsestraff 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 kan avbryta behandlingen av ett ärende, om ett ärende som har samband med det 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.

58 §

Beslut av kommissionen

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 ett ärende som gäller begäran om förhandsavgörande till Helsingfors förvaltningsdomstol för avgörande.

I förvaltningsdomstolens beslut får ändring sökas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

59 §

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

60 §

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.

61 §

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 sekretessen enligt 55 § 3 mom. och tystnadsplikten enligt 62 § 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.

62 §

Tystnadsplikt

Bestämmelser om tystnadsplikt och förbud mot utnyttjande av uppgifter finns i 23 § i lagen om offentlighet i myndigheternas verksamhet (621/1999).

11 kap.

Ikraftträdande och övergångsbestämmelser

63 §

Ikraftträdande

Denna lag träder i kraft den 1 januari 2019.

64 §

Övergångsbestämmelser

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

Helsingfors den 5 december 2018

Republikens President

Sauli Niinistö

Justitieminister Antti Häkkänen

UTGIVARE: JUSTITIEMINISTERIET ISSN 1456-9663