SUOMEN SÄÄDÖSKOKOELMA

Julkaistu Helsingissä 10 päivänä joulukuuta 2018

1054/2018

Laki

henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tätä lakia sovelletaan toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kyse on:

1) rikosten ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta;

2) syyteharkinnasta ja muusta rikokseen liittyvästä syyttäjän toiminnasta;

3) rikosasian käsittelemisestä tuomioistuimessa;

4) rikosoikeudellisen seuraamuksen täytäntöönpanemisesta;

5) yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä 1–4 kohdassa tarkoitetun toiminnan yhteydessä.

Sen lisäksi, mitä 1 momentissa säädetään, tätä lakia sovelletaan:

1) Puolustusvoimien suorittamaan ja Puolustusvoimien lukuun suoritettavaan henkilötietojen käsittelyyn, kun tietoja käsitellään puolustusvoimista annetun lain (551/2007) 2 §:n 1 momentin 1 kohdassa, 2 kohdan a alakohdassa sekä 3 ja 4 kohdassa säädettyjen tehtävien hoitamiseksi;

2) poliisin suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa poliisilain (872/2011) 1 luvun 1 §:n 1 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen;

3) Rajavartiolaitoksen suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa rajavartiolain (578/2005) 3 §:n 2 ja 3 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen.

Edellä 2 momentissa tarkoitettuun henkilötietojen käsittelyyn ei kuitenkaan sovelleta 10 §:n 2 momenttia henkilötietojen siirtämisestä Euroopan unionissa sijaitsevalle vastaanottajalle, 54 §:ää keskinäisestä avunannosta toisen EU:n jäsenvaltion kanssa eikä 7 lukua henkilötietojen siirrosta kolmansiin maihin ja kansainvälisille järjestöille.

HE 31/2018
HaVM 14/2018
EV 113/2018

Euroopan parlamentin ja neuvoston direktiivi 2016/680/EU (320160680); EUVL L 119, 4.5.2016, s. 89

Tätä lakia sovelletaan kuitenkin vain sellaiseen 1 ja 2 momentissa tarkoitettuun henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista tai jossa käsiteltävät tiedot muodostavat tai niiden on tarkoitus muodostaa rekisteri tai sen osa.

Tällä lailla pannaan täytäntöön luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, jäljempänä *rikosasioiden tietosuojadirektiivi*.

2 §

Suhde muuhun lainsäädäntöön

Jos muussa laissa on tästä laista poikkeavia säännöksiä, niitä sovelletaan tämän lain asemesta.

Oikeuteen saada tieto ja muuhun henkilötietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan, mitä viranomaisten toiminnan julkisuudesta säädetään.

3 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *henkilötiedoilla* kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (*rekisteröity*) välittömästi tai välillisesti liittyviä tietoja;

2) *käsittelyllä* tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista sekä muuta toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin;

3) *käsittelyn rajoittamisella* tallennettujen henkilötietojen merkitsemistä tarkoituksena rajoittaa niiden myöhempää käsittelyä;

4) *rekisterillä* jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, riippumatta siitä, onko tietojoukko keskitetty, hajautettu taikka toiminnallisin tai maantieteellisin perustein jaettu;

5) *toimivaltaisella viranomaisella* viranomaisia, joiden toimivalta kattaa rikosten ennalta estämisen, paljastamisen, selvittämisen tai syyteharkintaan saattamisen, syyteharkinnan tai muun rikoksesta syyttämiseen liittyvän toiminnan, rikosoikeudellisiin seuraamuksiin tuomitsemisen tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy, samoin kuin Puolustusvoimia, poliisia ja Rajavartiolaitosta näiden hoitaessa 1 §:n 2 momentissa tarkoitettuja tehtäviä;

6) *rekisterinpitäjällä* toimivaltaista viranomaista, joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai jonka tehtäväksi rekisterinpito on lailla säädetty;

7) *henkilötietojen käsittelijällä* luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun;

8) *vastaanottajalla* luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja;

9) *henkilötietojen tietoturvaloukkauksella* tietoturvallisuuden loukkausta, josta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai oikeudeton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin;

10) *asianmukaisilla suojatoimenpiteillä* sellaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan henkilötietojen käsittelyn lainmukaisuus, kun otetaan huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin kohdistuvat riskit;

11) *profiloinnilla* henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön henkilökohtaisia ominaisuuksia;

12) *geneettisillä tiedoilla* henkilötietoja, jotka koskevat sellaisia luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta, ja jotka on saatu kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla tai muutoin;

13) *biometrisillä tiedoilla* luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa;

14) *terveyttä koskevilla tiedoilla* luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, jotka ilmaisevat hänen terveydentilansa;

15) *kolmannella maalla* muuta valtiota kuin Euroopan unionin (EU) jäsenvaltiota, Euroopan talousalueeseen kuuluvaa valtiota tai Sveitsiä;

16) *kansainvälisellä järjestöllä* sellaista järjestöä ja sen alaisia elimiä, joihin sovelletaan kansainvälistä julkisoikeutta, sekä muuta elintä, joka on perustettu kahden tai useamman valtion välisellä sopimuksella tai tällaisen sopimuksen perusteella.

Mitä tässä laissa säädetään toimivaltaisesta viranomaisesta, sovelletaan myös 1 momentin 5 kohdassa tarkoitettua tehtävää hoitavaan yksityiseen.

Mitä tässä laissa säädetään EU:n jäsenvaltiosta, sovelletaan myös Euroopan talousalueeseen kuuluviin valtioihin ja Sveitsiin.

2 luku

Henkilötietojen käsittelyä koskevat periaatteet

4 §

Lainmukaisuusvaatimus

Henkilötietoja saa käsitellä vain, jos se on tarpeen laissa toimivaltaiselle viranomaiselle säädetyn, 1 §:n 1 tai 2 momentin alaan kuuluvan tehtävän suorittamiseksi.

Henkilötietoja on käsiteltävä asianmukaisesti ja huolellisesti.

5 §

Käyttötarkoitussidonnaisuus

Rekisterinpitäjä saa kerätä henkilötietoja vain tiettyjä nimenomaisia ja oikeutettuja tarkoituksia varten, eikä se saa käsitellä niitä kyseisten tarkoitusten kanssa yhteensopimattomalla tavalla.

Edellä 1 §:n 1 tai 2 momentissa säädettyä tarkoitusta varten kerättyjä henkilötietoja saa käsitellä muuhun kuin kyseisessä momentissa säädettyyn tarkoitukseen vain, jos käsittelystä säädetään laissa.

Henkilötietoja saa käsitellä 1 §:n 1 tai 2 momentissa säädettyyn tarkoitukseen myös yleisen edun mukaista arkistointia taikka tieteellistä, tilastollista tai historiallista tarkoitusta varten edellyttäen, että rekisteröidyn oikeuksia koskevat asianmukaiset suojatoimenpiteet on toteutettu.

6 §

Tarpeellisuusvaatimus

Käsiteltävien henkilötietojen on oltava käsittelyn tarkoituksen kannalta asianmukaisia ja tarpeellisia, eivätkä ne saa olla liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään. Tarpeettomat henkilötiedot on poistettava ilman aiheetonta viivytystä.

Henkilötiedot saa säilyttää muodossa, josta rekisteröity on tunnistettavissa, vain niin kauan kuin on tarpeen henkilötietojen käsittelyn tarkoituksen kannalta.

Henkilötietojen säilyttämisen tarpeellisuutta on arvioitava vähintään viiden vuoden välein, jollei henkilötietojen säilytysajoista muualla toisin säädetä.

7 §

Virheettömyysvaatimus

Käsiteltävien henkilötietojen on oltava täsmällisiä ja käsittelyn tarkoitus huomioon ottaen päivitettyjä. Rekisterinpitäjän on huolehdittava siitä, että kaikki kohtuulliset toimenpiteet on toteutettu sen varmistamiseksi, että käsittelyn tarkoituksiin nähden virheelliset tiedot poistetaan tai oikaistaan viipymättä.

8 §

Eräiden henkilötietojen erottaminen toisistaan

Rekisterinpitäjän on erotettava tarvittaessa ja mahdollisuuksien mukaan selvästi toisistaan henkilötiedot, jotka koskevat käsiteltävän asian kannalta eri asemassa olevia rekisteröityjä.

Tosiseikkoihin perustuvien henkilötietojen erottamiseksi henkilökohtaisiin arvioihin perustuvista henkilötiedoista on toteutettava kaikki kohtuulliset toimenpiteet.

9 §

Siirrettävien tai saataville asetettavien henkilötietojen laadun varmentaminen

Toimivaltaisen viranomaisen on toteutettava kaikki kohtuulliset toimenpiteet sen varmistamiseksi, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja siirretä eikä aseteta saataville.

Kaikkiin henkilötietojen siirtoihin on mahdollisuuksien mukaan lisättävä sellaiset tiedot, joiden avulla vastaanottava toimivaltainen viranomainen voi arvioida henkilötietojen paikkansapitävyyttä, täydellisyyttä, luotettavuutta ja ajantasaisuutta.

Jos ilmenee, että on siirretty virheellisiä henkilötietoja tai että henkilötietoja on siirretty lainvastaisesti, on asiasta viipymättä ilmoitettava vastaanottajalle. Vastaanottajan on asiasta tiedon saatuaan oikaistava tai poistettava henkilötiedot tai rajoitettava niiden käsittelyä.

10 §

Ilmoittamisvelvollisuus käsittelyn erityisistä edellytyksistä

Jos henkilötietojen käsittelyyn liittyy laissa säädettyjä erityisiä edellytyksiä, toimivaltaisen viranomaisen on henkilötietojen luovutuksen tai siirron yhteydessä ilmoitettava henkilötietojen vastaanottajalle kyseisistä edellytyksistä sekä velvollisuudesta noudattaa niitä.

Kun toimivaltainen viranomainen siirtää henkilötietoja EU:ssa sijaitsevalle vastaanottajalle, se ei saa asettaa henkilötietojen käsittelylle tiukempia edellytyksiä kuin mitä sovelletaan kansallisesti samankaltaisiin tiedonsiirtoihin.

11 §

Erityisiä henkilötietoryhmiä koskeva käsittely

Erityisiin henkilötietoryhmiin kuuluvia tietoja ovat henkilötiedot, joista ilmenee etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiliiton jäsenyys, sekä geneettiset tiedot, luonnollisen henkilön yksiselitteiseen tunnistamiseen tarkoitetut biometriset tiedot sekä terveyttä taikka luonnollisen henkilön seksuaalista käyttäytymistä ja seksuaalista suuntautumista koskevat tiedot.

Edellä 1 momentissa tarkoitettujen henkilötietojen käsittely on sallittu vain, jos se on välttämätöntä, rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu ja jos:

1) käsittelystä säädetään laissa;
2) kyse on rikosasian käsittelystä syyttäjäntoimessa tai tuomioistuimessa;
3) rekisteröidyn tai toisen luonnollisen henkilön elintärkeän edun suojaaminen edellyttää sitä; tai
4) käsittely koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi.

Sellainen profilointi, joka johtaa erityisiin henkilötietoryhmiin perustuvaan luonnollisten henkilöiden syrjintään, on kielletty.

12 §

Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä vain, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:

1) toimivaltaisen viranomaisen laissa säädetyn tehtävän suorittamiseksi;
2) rekisteröidyn tai rekisterinpitäjän oikeuksien tai velvollisuuksien toteuttamiseksi; tai
3) 5 §:n 3 momentin mukaista historiallista tai tieteellistä tutkimusta taikka tilastointia varten.

Henkilötunnusta ei saa tarpeettomasti merkitä rekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

13 §

Automatisoidut yksittäispäätökset

Jollei laissa toisin säädetä, päätöstä ei saa tehdä pelkästään automatisoidun henkilötietojen käsittelyn perusteella, jos päätöksellä on rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai se on muutoin hänen kannaltaan merkittävä.

3 luku

Rekisterinpitäjä ja henkilötietojen käsittelijä

14 §

Rekisterinpitäjän vastuu

Rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään lainmukaisesti. Sen on lisäksi kyettävä osoittamaan, että henkilötietoja on käsitelty 2 luvun mukaisesti.

Rekisterinpitäjän on toteutettava tarvittavat 1 momentissa säädetyn vastuun edellyttämät tekniset ja organisatoriset toimenpiteet. Toimenpiteiden toteuttamisessa on otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin kohdistuvat riskit.

15 §

Sisäänrakennettu ja oletusarvoinen tietosuoja

Rekisterinpitäjän tulee sekä henkilötietojen käsittelytapoja määrittäessään että henkilötietojen käsittelyn yhteydessä toteuttaa asianmukaiset tekniset ja organisatoriset suojatoimenpiteet käsittelyn lainmukaisuuden ja rekisteröidyn oikeuksien suojelemisen varmistamiseksi. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset ratkaisut, toimenpiteiden toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset samoin kuin ne riskit, jotka käsittely henkilön oikeuksille aiheuttaa.

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen, että oletusarvoisesti käsitellään vain kunkin erityisen käsittelytarkoituksen kannalta tarpeellisia henkilötietoja.

16 §

Yhteisrekisterinpitäjät

Jos kaksi tai useampi rekisterinpitäjä määrittää yhdessä käsittelyn tarkoitukset ja keinot, niiden on sovittava keskinäisestä vastuunjaostaan tämän lain mukaisten velvollisuuksien hoitamisessa, jollei vastuunjaosta ole säädetty laissa.

Edellä 1 momentissa tarkoitettujen rekisterinpitäjien on nimettävä keskuudestaan yhteyspisteenä toimiva rekisterinpitäjä, johon rekisteröity voi olla yhteydessä oikeuksiensa käyttöä koskevissa asioissa. Rekisteröity voi kuitenkin käyttää tämän lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään.

17 §

Henkilötietojen käsittelijä

Henkilötietoja rekisterinpitäjän lukuun käsittelevän on annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoinkin riittävät takeet niistä organisatorisista ja teknisistä toimenpiteistä, joilla se varmistaa, että henkilötietoja käsitellään tässä laissa säädettyjen vaatimusten mukaisesti.

Henkilötietojen käsittelijä tai sen palveluksessa oleva ei saa käsitellä henkilötietoja muutoin kuin rekisterinpitäjän ohjeiden mukaisesti, eikä siirtää henkilötietojen käsittelyä toiselle käsittelijälle ilman rekisterinpitäjän kirjallista lupaa.

Henkilötietojen käsittelijän suorittamasta henkilötietojen käsittelystä on tehtävä kirjallinen sopimus tai annettava kirjallinen määräys, josta ilmenevät käsiteltävät henkilötiedot, käsittelyn kesto, luonne ja tarkoitus, käsiteltävät henkilötietoryhmät ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. Edellä tarkoitetussa kirjallisessa asiakirjassa on lisäksi määrättävä, että henkilötietojen käsittelijä:

1) toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti;

2) varmistaa, että henkilötietoja käsittelevät luonnolliset henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai että heitä sitoo lakisääteinen salassapitovelvollisuus;

3) avustaa rekisterinpitäjää kaikin tarkoituksenmukaisin tavoin, jotta voidaan varmistaa, että rekisteröidyn oikeuksia koskevia säännöksiä noudatetaan;

4) rekisterinpitäjän valinnan mukaan poistaa taikka palauttaa tietojenkäsittelypalveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos laissa toisin säädetään;

5) saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tämän pykälän noudattamisen osoittamiseksi;

6) täyttää tässä pykälässä tarkoitetut toisen käsittelijän käyttöä koskevat edellytykset.

18 §

Seloste käsittelytoimista

Rekisterinpitäjän on ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä kirjallista selostetta, jossa on seuraavat tiedot:

1) rekisterinpitäjän ja tarvittaessa yhteisrekisterinpitäjän sekä 38 §:ssä tarkoitetun tietosuojavastaavan nimi ja yhteystiedot;
2) henkilötietojen käsittelyn tarkoitukset ja oikeudellinen peruste;
3) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja käsiteltävistä henkilötietoryhmistä;
4) vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan;
5) kolmanteen maahan tai kansainväliselle järjestölle suoritettujen henkilötietojen siirtojen ryhmät;
6) mahdollisuuksien mukaan eri henkilötietoryhmien poistamisen suunnitellut määräajat;
7) mahdollinen profiloinnin käyttö;
8) mahdollisuuksien mukaan yleinen kuvaus tietojärjestelmistä ja niiden suojauksen periaatteista sekä yleinen kuvaus 31 §:ssä tarkoitetuista teknisistä ja organisatorisista turvatoimista.

Henkilötietojen käsittelijän on ylläpidettävä kaikesta rekisterinpitäjän lukuun suoritettavasta henkilötietojen käsittelystä kirjallista selostetta, jossa on seuraavat tiedot:

1) henkilötietojen käsittelijän tai käsittelijöiden sekä tietosuojavastaavan nimi ja yhteystiedot;
2) kunkin rekisterinpitäjän, jonka lukuun käsittelijä toimii, nimi ja yhteystiedot;
3) kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät;
4) jos rekisterinpitäjä on nimenomaisesti niin ohjeistanut, mahdolliset tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle;
5) mahdollisuuksien mukaan yleinen kuvaus 31 §:ssä tarkoitetuista teknisistä ja organisatorisista suojatoimenpiteistä.

19 §

Lokitiedot

Rekisterinpitäjän ja henkilötietojen käsittelijän on huolehdittava lokitietojen säilyttämisestä automaattisessa tietojenkäsittelyjärjestelmässään suoritetusta henkilötietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta, siirtämisestä, yhdistämisestä ja poistamisesta. Kyselyjä ja luovutuksia koskevien lokitietojen avulla on pystyttävä selvittämään kyselyn ja luovutuksen peruste, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys.

Lokitietoja saa käyttää ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, sisäiseen valvontaan, henkilötietojen eheyden ja turvallisuuden varmistamiseen sekä rikosoikeudellisiin menettelyihin.

20 §

Tietosuojaa koskeva vaikutustenarviointi

Rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista arvioitava suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojaan.

Rekisterinpitäjän on tehtävä kirjallinen vaikutustenarviointi, jos suunniteltu henkilötietojen käsittely saattaa aiheuttaa merkittävän riskin luonnollisen henkilön oikeuksien toteutumisen kannalta. Vaikutustenarvioon on sisällytettävä yleinen kuvaus suunnitelluista kä-

sittelytoimista, arvio rekisteröidyn oikeuksiin kohdistuvista riskeistä ja toimet niiden vähentämiseksi sekä toimet, joilla henkilötietojen suoja varmistetaan.

21 §

Tietosuojaviranomaisen ennakkokuuleminen

Rekisterinpitäjän tai henkilötietojen käsittelijän on kuultava tietosuojavaltuutettua ennen henkilötietojen käsittelyä, jos:

1) 20 §:n 2 momentissa tarkoitetun kirjallisen vaikutusarvioinnin mukaan suunnitelluista suojatoimenpiteistä huolimatta käsittely aiheuttaa merkittävän riskin rekisteröidyn oikeuksille; tai

2) tietojen käsittely erityisesti uusien tekniikoiden, mekanismien tai menettelyjen käyttämisen johdosta aiheuttaa merkittävän riskin rekisteröityjen oikeuksien kannalta.

Rekisterinpitäjän on toimitettava tietosuojavaltuutetulle 20 §:n 2 momentissa tarkoitettu vaikutustenarviointi ja pyynnöstä muut sellaiset tiedot, joiden avulla tietosuojavaltuutettu voi arvioida henkilötietojen käsittelyn lainmukaisuutta.

Jos tietosuojavaltuutettu katsoo, että 1 momentissa tarkoitettu käsittely muodostuisi tämän lain vastaiseksi, tietosuojavaltuutetun tulee antaa kuuden viikon kuluessa kuulemispyynnön vastaanottamisesta rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle ohjausta käsittelyn saattamiseksi lainmukaiseksi. Määräaikaa voidaan jatkaa kuukaudella, jos suunnitellun käsittelyn monimutkaisuus sitä edellyttää. Tietosuojavaltuutetun on ilmoitettava rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle määräajan jatkamisesta sekä viivästymisen syistä kuukauden kuluessa kuulemispyynnön vastaanottamisesta.

4 luku

Rekisteröidyn oikeudet

22 §

Tietosuojaseloste ja ilmoitusvelvollisuus

Rekisterinpitäjän on ylläpidettävä sen vastuulle kuuluvasta henkilötietojen käsittelystä kirjallista selostetta, joka on asetettava julkisesti saataville ja jossa on ainakin seuraavat tiedot:

1) rekisterinpitäjän ja tietosuojavastaavan yhteystiedot sekä, jos rekisterinpitäjä katsoo sen tarpeelliseksi, tietosuojavastaavan nimi;

2) yhteisrekisterinpitäjien yhteyspisteenä toimivan rekisterinpitäjän nimi ja yhteystiedot sekä tieto siitä, että rekisteröity voi käyttää tämän lain mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään;

3) henkilötietojen käsittelyn tarkoitukset ja oikeusperuste;

4) henkilötietojen säilytysaika, tai jos sitä ei ole määritelty, säilytysajan määrittämiskriteerit;

5) mahdolliset henkilötietojen säännönmukaiset vastaanottajat tai vastaanottajaryhmät;

6) tieto siitä, että rekisteröidyllä on oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista;

7) tieto siitä, että rekisteröidyllä on oikeus tehdä 56 §:ssä tarkoitettu toimenpidepyyntö tietosuojavaltuutetulle, ja valtuutetun yhteystiedot.

Rekisterinpitäjän on annettava rekisteröidylle 1 momentissa tarkoitettu seloste ja muut tarpeelliset tiedot tässä luvussa säädettyjen rekisteröidyn oikeuksien käyttämiseksi, jos

näiden tietojen antaminen on yksittäistapauksessa tarpeen mainittujen oikeuksien käyttämisen mahdollistamiseksi. Rekisterinpitäjä voi jättää tiedot antamatta kokonaan tai osittain, jos se on välttämätöntä 28 §:ssä mainituilla perusteilla.

23 §

Rekisteröidyn tarkastusoikeus

Jokaisella on oikeus saada rekisterinpitäjältä tieto siitä, käsitelläänkö häntä koskevia henkilötietoja. Jos kyseisiä tietoja käsitellään, rekisteröidyllä on oikeus saada rekisterinpitäjältä seuraavat tiedot:

1) käsiteltävät henkilötiedot ja kaikki tietojen alkuperästä käytettävissä olevat tiedot;
2) käsittelyn tarkoitukset ja oikeusperuste;
3) käsittelyn kohteena olevat henkilötietoryhmät;
4) vastaanottajat tai vastaanottajaryhmät, joille rekisteröidyn henkilötietoja on luovutettu;
5) henkilötietojen säilytysaika, tai jos sitä ei ole määritelty, säilytysajan määrittämiskriteerit;
6) rekisteröidyn oikeus vaatia rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista, poistamista tai niiden käsittelyn rajoittamista;
7) rekisteröidyn oikeus tehdä 56 §:ssä tarkoitettu toimenpidepyyntö tietosuojavaltuutetulle ja valtuutetun yhteystiedot.

Se, joka haluaa tarkastaa itseään koskevat tiedot 1 momentissa tarkoitetulla tavalla, voi esittää tätä tarkoittavan pyynnön rekisterinpitäjälle omakätisesti allekirjoitetulla asiakirjalla tai sitä vastaavalla varmennetulla tavalla tai henkilökohtaisesti rekisterinpitäjän luona.

24 §

Tarkastusoikeuden rajoitukset

Rekisteröidyn tarkastusoikeutta voidaan kokonaan tai osittain lykätä tai rajoittaa tai se voidaan evätä siltä osin kuin se on välttämätöntä 28 §:ssä mainituilla perusteilla. Jos rekisteröidyn tarkastusoikeutta lykätään, rajoitetaan tai se evätään, rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava siitä rekisteröidylle kirjallisella todistuksella. Myös lykkäämisen, rajoittamisen ja epäämisen perustelut on ilmoitettava, paitsi jos niiden ilmoittaminen vaarantaisi epäämisen tai rajoittamisen tarkoituksen. Tarkastusoikeuden epäämisenä pidetään myös sitä, että rekisterinpitäjä ei ole kolmen kuukauden kuluessa pyynnön esittämisestä antanut kirjallista vastausta rekisteröidylle.

Rekisterinpitäjän on ilmoitettava rekisteröidylle tämän oikeudesta tehdä toimenpidepyyntö tietosuojavaltuutetulle tarkastusoikeuden lykkäämisen, rajoittamisen tai epäämisen johdosta sekä oikeudesta käyttää tarkastusoikeutta 29 §:n mukaisesti tietosuojavaltuutetun välityksellä.

Rekisterinpitäjän on säilytettävä tieto niistä perusteista, joihin tarkastusoikeuden epääminen tai rajoittaminen perustuu.

25 §

Henkilötietojen oikaiseminen, poistaminen ja käsittelyn rajoittaminen

Rekisterinpitäjän on oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheetonta viivytystä oikaistava tai täydennettävä rekisteröityä koskeva, käsittelyn tarkoituksen kannalta virheellinen tai puutteellinen henkilötieto.

Rekisterinpitäjän on oma-aloitteisesti tai rekisteröidyn vaatimuksesta ilman aiheetonta viivytystä poistettava rekisteröityä koskevat henkilötiedot, jos niiden käsittely on vastoin

4 tai 5 §:n, 6 §:n 1 tai 2 momentin taikka 7 tai 11 §:n säännöksiä. Poistamisen sijasta rekisterinpitäjän on kuitenkin rajoitettava käsittelyä, jos:

1) rekisteröity kiistää tietojen paikkansapitävyyden eikä niiden paikkansapitävyyttä tai virheellisyyttä voida todentaa; tai

2) henkilötiedot on säilytettävä todistelua varten.

Jos käsittelyä on rajoitettu 2 momentin 1 kohdan nojalla, rekisterinpitäjän on ennen rajoituksen poistamista ilmoitettava siitä rekisteröidylle.

26 §

Rekisteröidyn vaatimuksen epääminen

Jollei rekisterinpitäjä hyväksy rekisteröidyn vaatimusta henkilötietojen oikaisemisesta, täydentämisestä, poistamisesta tai niiden käsittelyn rajoittamisesta, rekisterinpitäjän on ilmoitettava rekisteröidylle kirjallisella todistuksella kieltäytymisestä ja sen perusteista. Tiedot kieltäytymisen perusteista voidaan kokonaan tai osittain jättää antamatta siltä osin kuin se on välttämätöntä 28 §:ssä mainituilla perusteilla.

Rekisterinpitäjän on ilmoitettava rekisteröidylle tämän oikeudesta tehdä toimenpidepyyntö tietosuojavaltuutetulle 1 momentissa tarkoitetun kieltäytymisen johdosta sekä oikeudesta käyttää 25 §:ssä tarkoitettuja oikeuksia 29 §:n mukaisesti tietosuojavaltuutetun välityksellä.

27 §

Rekisterinpitäjän velvollisuus ilmoittaa oikaisemisesta, poistamisesta tai käsittelyn rajoittamisesta

Rekisterinpitäjän on ilmoitettava virheellisten henkilötietojen oikaisemisesta sille viranomaiselle, jolta virheelliset henkilötiedot ovat peräisin.

Jos henkilötietoja on oikaistu tai poistettu taikka niiden käsittelyä on rajoitettu 25 §:n nojalla, rekisterinpitäjän on ilmoitettava asiasta niille vastaanottajille, joille rekisterinpitäjä on luovuttanut kyseisiä tietoja. Vastaanottajan on oikaistava tai poistettava sillä olevat kyseiset henkilötiedot taikka rajoitettava niiden käsittelyä.

28 §

Rekisteröidyn oikeuksien rajoittaminen

Rekisteröidyn oikeuksia voidaan rajoittaa 22 §:n 2 momentissa, 24 §:n 1 momentissa, 26 §:n 1 momentissa ja 35 §:ssä tarkoitetulla tavalla, jos se rekisteröidyn oikeudet huomioon ottaen on oikeasuhtaista ja välttämätöntä:

1) rikosten ennalta estämiselle, paljastamiselle, selvittämiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle aiheutuvan haitan välttämiseksi;

2) viranomaisen muun tutkinnan, selvityksen tai vastaavan menettelyn turvaamiseksi;

3) yleisen turvallisuuden suojelemiseksi;

4) kansallisen turvallisuuden suojelemiseksi; tai

5) muiden henkilöiden oikeuksien suojelemiseksi.

29 §

Oikeuksien käyttäminen tietosuojavaltuutetun välityksellä

Rekisteröidyllä on oikeus pyytää tietosuojavaltuutettua tarkastamaan henkilötietojen ja niiden käsittelyn lainmukaisuus, jos tämän tai muun lain nojalla rekisteröidyn tarkastusoikeutta on lykätty, rajoitettu tai evätty tai jos rekisterinpitäjä ei hyväksy rekisteröidyn vaa-

timusta henkilötietojen oikaisemisesta, täydentämisestä, poistamisesta tai niiden käsittelyn rajoittamisesta.

Jos rekisteröity käyttää 1 momentissa tarkoitettua oikeuttaan, tietosuojavaltuutetun on kohtuullisen ajan kuluessa ilmoitettava rekisteröidylle toimenpiteistä, joihin se on ryhtynyt. Tietosuojavaltuutetun on myös ilmoitettava rekisteröidylle hänen oikeudestaan tehdä tietosuojavaltuutetulle 56 §:ssä tarkoitettu toimenpidepyyntö.

30 §

Rekisteröidyn oikeuksien käytön edistäminen ja toimenpiteiden maksuttomuus

Rekisterinpitäjän on edistettävä rekisteröityjen mahdollisuuksia käyttää tässä luvussa tarkoitettuja oikeuksia. Kaikki rekisteröidylle annettavat ilmoitukset ja henkilötietojen käsittelyä koskevat tiedot on annettava tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Rekisteröidylle tämän lain mukaisesti annettavat ilmoitukset ja tiedot sekä rekisteröidyn tämän lain mukaisesti tekemien pyyntöjen käsitteleminen ovat rekisteröidylle maksuttomia. Jos rekisteröidyn pyynnöt ovat niiden toistuvuudesta tai muusta syystä ilmeisen kohtuuttomia tai perusteettomia, rekisterinpitäjä voi kuitenkin periä toimenpiteestä maksun. Maksun määrän perusteista säädetään valtion maksuperustelaissa (150/1992).

Jos rekisterinpitäjä perii maksun 2 momentin nojalla, sen on tarvittaessa osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

5 luku

Tietoturvallisuus

31 §

Henkilötietojen suojaaminen

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee teknisin ja organisatorisin toimenpitein huolehtia henkilötietojen riittävästä suojaamisesta ottaen huomioon käsittelystä rekisteröidyn oikeuksille aiheutuva riski. Henkilötiedot on erityisesti suojattava oikeudettomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta. Toimenpiteitä suunniteltaessa ja toteutettaessa tulee ottaa huomioon:

1) uusin tekniikka;
2) toimenpiteiden toteuttamiskustannukset;
3) käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset;
4) luonnollisen henkilön oikeuksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

32 §

Henkilötietojen suojaaminen automatisoidussa käsittelyssä

Sen lisäksi, mitä 31 §:ssä säädetään, automatisoidun käsittelyn osalta rekisterinpitäjän tai henkilötietojen käsittelijän on toteutettava riskien arvioinnin pohjalta toimenpiteet, joiden tarkoituksena on:

1) evätä asiattomilta pääsy käsittelyyn käytettäviin laitteisiin;
2) estää tietovälineiden luvaton lukeminen, jäljentäminen, muuttaminen ja poistaminen;
3) estää henkilötietojen luvaton syöttäminen järjestelmään sekä järjestelmään tallennettujen henkilötietojen luvaton tarkastelu, muuttaminen ja poistaminen;

4) estää asiattomia käyttämästä automatisoituja käsittelyjärjestelmiä tiedonsiirtolaitteiden avulla;

5) varmistaa, että automatisoidun käsittelyjärjestelmän käyttöön oikeutetut henkilöt pääsevät ainoastaan käyttöoikeuksiensa piiriin kuuluviin henkilötietoihin;

6) varmistaa, että on mahdollista tarkastaa ja todeta, mille tahoille henkilötietoja on siirretty tai asetettu saataville tai voidaan siirtää tai asettaa saataville tiedonsiirtolaitteiden avulla;

7) varmistaa, että jälkikäteen on mahdollista tarkistaa ja todeta, mitä henkilötietoja on syötetty automatisoituihin käsittelyjärjestelmiin, milloin niitä on syötetty ja kuka niitä on syöttänyt;

8) estää henkilötietojen oikeudeton lukeminen, jäljentäminen, muuttaminen ja poistaminen tietoja siirrettäessä tai tietovälineitä kuljetettaessa;

9) varmistaa, että käytetyt järjestelmät voidaan häiriön tapahtuessa palauttaa entiselleen;

10) varmistaa, että järjestelmä toimii, havaituista toimintojen virheistä ilmoitetaan ja järjestelmän toimintahäiriö ei voi vahingoittaa tallennettuja henkilötietoja.

33 §

Henkilötietojen käsittelijän velvollisuus ilmoittaa tietoturvaloukkauksesta

Henkilötietojen käsittelijän on henkilötietojen tietoturvaloukkauksesta tiedon saatuaan ilman aiheetonta viivytystä ilmoitettava loukkauksesta rekisterinpitäjälle.

34 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetulle

Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetulle, paitsi jos loukkauksesta ei todennäköisesti aiheudu vaaraa rekisteröidyn oikeuksille.

Rekisterinpitäjän on tehtävä 1 momentissa tarkoitettu ilmoitus ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa saatuaan tietoturvaloukkauksen tietoonsa. Jos ilmoitus tietosuojavaltuutetulle tehdään tätä myöhemmin, ilmoituksessa on kerrottava viivytyksen syyt.

Rekisterinpitäjän on säilytettävä tiedot tietoturvaloukkauksista ja niihin liittyvistä seikoista, niiden vaikutuksista ja toteutetuista korjaavista toimenpiteistä.

35 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta rekisteröidylle

Rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisteröidylle, jos tietoturvaloukkaus todennäköisesti aiheuttaa merkittävän riskin rekisteröidyn oikeuksille. Ilmoittamisvelvollisuutta ei kuitenkaan ole, jos:

1) rekisterinpitäjä on toteuttanut loukkauksen kohteena oleviin henkilötietoihin niiden väärinkäyttöä tehokkaasti estäviä asianmukaisia teknisiä ja organisatorisia suojatoimenpiteitä; tai

2) rekisterinpitäjä on loukkauksen jälkeen ryhtynyt toimenpiteisiin sen varmistamiseksi, ettei loukkaus todennäköisesti aiheuta riskiä rekisteröidyn oikeuksien toteutumiselle.

Rekisterinpitäjä voi rekisteröidylle tehtävän ilmoituksen sijasta tiedottaa tietoturvaloukkauksesta julkisella ilmoituksella, jos ilmoituksen tekeminen rekisteröidyille vaatisi kohtuutonta vaivaa.

Rekisteröidylle ilmoittamista voidaan lykätä tai rajoittaa tai se voidaan jättää tekemättä, jos 28 §:n mukaiset edellytykset täyttyvät.

36 §

Rekisterinpitäjän velvollisuus ilmoittaa tietoturvaloukkauksesta toiselle rekisterinpitäjälle

Rekisterinpitäjän on ilman aiheetonta viivytystä ilmoitettava henkilötietojen tietoturvaloukkauksesta sellaiselle Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle, jonka toimittamiin tai jolle toimitettuihin tietoihin loukkaus kohdistuu.

37 §

Tietoturvaloukkauksesta annettavan ilmoituksen sisältö

Edellä 34 §:ssä tarkoitetussa ilmoituksessa tietosuojavaltuutetulle ja 36 §:ssä tarkoitetussa ilmoituksessa Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle on kuvattava henkilötietojen tietoturvaloukkaus. Kuvaukseen on mahdollisuuksien mukaan sisällytettävä tiedot asianomaisten rekisteröityjen ryhmistä, rekisteröityjen arvioidusta lukumäärästä, henkilötietotyyppien ryhmistä ja henkilötietojen arvioidusta lukumäärästä.

Edellä 35 §:ssä tarkoitetussa rekisteröidylle annettavassa ilmoituksessa on kuvattava tietoturvaloukkauksen luonne.

Edellä 1 ja 2 momentissa tarkoitetuista ilmoituksista on lisäksi käytävä ilmi:

1) tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

2) tietoturvaloukkauksen todennäköiset seuraukset;

3) toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tietoturvaloukkauksen johdosta ja tarvittaessa toimenpiteet sen haittavaikutusten lieventämiseksi.

Tietosuojavaltuutetulle ja Suomessa tai toisessa EU:n jäsenvaltiossa sijaitsevalle rekisterinpitäjälle annettavat tiedot voidaan toimittaa vaiheittain siltä osin kuin niitä ei ole mahdollista toimittaa samanaikaisesti.

6 luku

Tietosuojavastaava

38 §

Tietosuojavastaavan nimeäminen

Rekisterinpitäjän on nimettävä tietosuojavastaava. Tietosuojavastaavalla on oltava riittävä asiantuntemus henkilötietojen käsittelyä koskevasta lainsäädännöstä ja alan käytänteistä sekä valmiudet hoitaa 40 §:ssä tarkoitetut tehtävät. Yksi tietosuojavastaava voidaan nimetä useaa toimivaltaista viranomaista varten, jos se on perusteltua viranomaisten organisaatiorakenne ja koko huomioon ottaen.

Rekisterinpitäjän on ilmoitettava tietosuojavastaavan yhteystiedot tietosuojavaltuutetulle.

39 §

Tietosuojavastaavan asema

Rekisterinpitäjän on otettava tietosuojavastaava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn.

Rekisterinpitäjän on turvattava tietosuojavastaavan toimintaedellytykset tälle 40 §:ssä säädettyjen tehtävien hoitamiseksi sekä annettava pääsy henkilötietoihin ja käsittelytoimiin.

40 §

Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtävänä on:

1) neuvoa rekisterinpitäjää ja henkilötietoja sen palveluksessa käsitteleviä henkilötietojen suojaa koskevissa asioissa;

2) valvoa henkilötietojen käsittelyä koskevan sääntelyn ja rekisterinpitäjän henkilötietojen käsittelyyn liittyvien menettelytapojen noudattamista;

3) antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa, että se toteutetaan 20 §:ssä säädetyn mukaisesti;

4) tehdä yhteistyötä tietosuojavaltuutetun kanssa ja toimia sen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietosuojavastaavan tehtävät eivät ulotu tuomioistuinten lainkäyttötoimintaan eikä valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen laillisuusvalvontaan.

7 luku

Henkilötietojen siirrot kolmansiin maihin ja kansainvälisille järjestöille

41 §

Henkilötietojen siirtoja koskevat yleiset periaatteet

Toimivaltainen viranomainen saa siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos tässä laissa tarkoitettuun henkilötietojen käsittelyyn sovellettavia muita säännöksiä noudatetaan ja:

1) siirto on tarpeen 1 §:n 1 momentissa mainittua tarkoitusta varten;

2) henkilötiedot siirretään kolmannen maan rekisterinpitäjälle tai kansainväliselle järjestölle, joka on toimivaltainen käsittelemään henkilötietoja 1 §:n 1 momentissa mainitussa tarkoituksessa; ja

3) tietosuojan riittävyydestä on rikosasioiden tietosuojadirektiivin 36 artiklassa tarkoitettu Euroopan komission (*komissio*) voimassa oleva päätös tai jollei tällaista päätöstä ole tehty, asianmukaiset suojatoimet ovat olemassa tämän lain 42 §:n mukaisesti, tai jos 43 §:ssä säädetyt erityistilanteita koskevat poikkeukset tulevat sovellettaviksi.

Jos henkilötiedot on saatu toisesta EU:n jäsenvaltiosta, siirron edellytyksenä on lisäksi, että kyseinen jäsenvaltio on antanut siirrolle luvan. Siirto, joka tehdään ilman tällaista lupaa, on sallittu vain, jos se on välttämätön jonkin valtion yleiseen turvallisuuteen tai EU:n jäsenvaltion olennaisiin etuihin kohdistuvan välittömän ja vakavan uhan estämiseksi, eikä lupaa voida saada ajoissa. Siirrosta on ilmoitettava viipymättä ennakkoluvan antamisesta vastaavalle viranomaiselle.

Jos henkilötiedot siirretään edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle, alkuperäisen siirron toteuttanut toimivaltainen viranomainen voi antaa luvan edelleen siirtämiselle noudattaen 1 ja 2 momenttia ja ottaen asianmukaisesti huomioon rikoksen vakavuuden, henkilötietojen alkuperäisen siirron tarkoituksen ja henkilötietojen suojan tason siinä kolmannessa maassa tai kansainvälisessä järjestössä, johon tai jolle tiedot siirretään edelleen sekä muut merkittävät seikat.

42 §

Siirto asianmukaisten suojatoimien perusteella

Jos komissio ei ole tehnyt 41 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä, henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle, jos muut 41 §:ssä säädetyt edellytykset täyttyvät, ja:

1) oikeudellisesti sitovassa asiakirjassa määrätään asianmukaisista henkilötietojen suojatoimista; tai

2) rekisterinpitäjä kaikkia henkilötietojen siirtämiseen liittyviä seikkoja arvioituaan katsoo, että henkilötietojen suojaamiseksi on toteutettu asianmukaiset suojatoimet.

Rekisterinpitäjän on ilmoitettava tietosuojavaltuutetulle 1 momentin 2 kohdan perusteella tehtyjen siirtojen sarjat. Siirroista on säilytettävä seuraavat tiedot ja ne on asetettava pyynnöstä tietosuojavaltuutetun saataville:

1) siirtojen päivämäärät ja ajankohdat;
2) vastaanottava toimivaltainen viranomainen;
3) siirtojen perusteet; ja
4) siirretyt henkilötiedot.

43 §

Erityistilanteita koskevat poikkeukset

Jos komissio ei ole tehnyt 41 §:n 1 momentin 3 kohdassa tarkoitettua päätöstä eivätkä 42 §:ssä säädetyt tiedonsiirron edellytykset täyty, henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle vain, jos siirto on välttämätön:

1) rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaamiseksi;
2) rekisteröidyn oikeutettujen ja merkitykseltään painavien etujen turvaamiseksi;
3) EU:n jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan estämiseksi; tai
4) yksittäistapauksessa 1 §:n 1 momentissa mainittuja tarkoituksia varten tai niihin liittyvien oikeusvaateiden laatimiseksi, esittämiseksi tai puolustamiseksi.

Henkilötietoja ei kuitenkaan saa siirtää 1 momentin 4 kohdan nojalla, jos asianomaisen rekisteröidyn oikeuksia on pidettävä siirtoa puoltavaa yleistä etua painavampana.

Siirroista, jotka perustuvat 1 momenttiin, on säilytettävä seuraavat tiedot ja ne on asetettava pyynnöstä tietosuojavaltuutetun saataville;

1) siirron päivämäärä ja ajankohta;
2) vastaanottava toimivaltainen viranomainen;
3) siirron peruste; ja
4) siirretyt henkilötiedot.

44 §

Henkilötietojen siirto kolmansiin maihin yksityisille ja muille vastaanottajille

Sen estämättä, mitä 41 §:n 1 momentin 2 kohdassa säädetään, toimivaltainen viranomainen voi yksittäisessä tapauksessa siirtää henkilötietoja suoraan kolmansiin maihin sijoittautuneille yksityisille ja muille vastaanottajille, jos tämän lain muita säännöksiä noudatetaan ja:

1) siirto on välttämätön, jotta siirron toteuttava toimivaltainen viranomainen voi hoitaa sille säädetyt 1 §:n 1 momentissa tarkoitetut tehtävänsä;

2) tietoja siirtävä toimivaltainen viranomainen katsoo, että asianomaisen rekisteröidyn oikeudet eivät syrjäytä yleistä etua, jonka perusteella siirto käsiteltävänä olevassa tapauksessa on tarpeen;

3) tietoja siirtävä toimivaltainen viranomainen katsoo, että siirto kolmannen maan toimivaltaiselle viranomaiselle olisi asian kiireellisyydestä tai muusta syystä tehoton tai epätarkoituksenmukainen;

4) kolmannen maan viranomaiselle, joka on toimivaltainen 1 §:n 1 momentin mukaisissa tarkoituksissa, ilmoitetaan siirrosta ilman aiheetonta viivästystä, jollei se olisi tehotonta tai epätarkoituksenmukaista;

5) tietoja siirtävä toimivaltainen viranomainen ilmoittaa vastaanottajalle, mitä tiettyä tarkoitusta tai tiettyjä tarkoituksia varten tämä saa käsitellä henkilötietoja, että käsittelyn on oltava välttämätöntä näitä tarkoituksia varten, ja että tietoja ei saa käsitellä muita tarkoituksia varten; ja

6) siirto ei ole vastoin Suomen kansainvälisiä sopimusvelvoitteita.

Tiedot siirtävän toimivaltaisen viranomaisen on säilytettävä tiedot 1 momentin nojalla tehtävästä siirrosta ja ilmoitettava siirrosta tietosuojavaltuutetulle.

8 luku

Valvontaviranomainen

45 §

Tietosuojavaltuutettu

Tämän lain noudattamista valvoo tietosuojalain (1050/2018) 8 §:ssä tarkoitettu tietosuojavaltuutettu.

Tämän lain säännöksiä valvonnasta ei sovelleta tuomioistuimeen, valtioneuvoston oikeuskansleriin eikä eduskunnan oikeusasiamieheen.

Tietosuojavaltuutettu on itsenäinen ja riippumaton hoitaessaan tässä laissa säädettyjä tehtäviään.

46 §

Tehtävät

Tietosuojavaltuutetun tehtäviin kuuluu tämän lain noudattamisen valvomisen lisäksi:

1) edistää yleistä tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, lainsäädännöstä, suojatoimista ja oikeuksista;

2) edistää rekisterinpitäjien ja henkilötietojen käsittelijöiden tietoisuutta niille tämän lain mukaan kuuluvista velvollisuuksista;

3) antaa pyynnöstä rekisteröidyille tietoja heille tämän lain nojalla kuuluvien oikeuksien käyttämisestä;

4) antaa neuvontaa 21 §:ssä tarkoitetussa ennakkokuulemisessa;

5) tehdä selvityksiä tämän lain noudattamisesta;

6) tarkistaa 29 §:n mukaisesti käsittelyn lainmukaisuus;

7) käsitellä rekisteröidyn ja 56 §:ssä tarkoitetun yhteisön tekemiä toimenpidepyyntöjä;

8) seurata henkilötietojen suojaan vaikuttavaa teknologista ja muuta kehitystä.

Tietosuojavaltuutetun tehtävänä on lisäksi osallistua luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/67968 artiklassa tarkoitetun tietosuojaneuvoston toimintaan. Tietosuojavaltuutettu ei kuitenkaan vie tietosuojaneuvoston käsiteltäväksi asiaa, jossa on kyse henkilötietojen käsittelystä 1 §:n 2 momentissa tarkoitetun toiminnan yhteydessä.

Tietosuojavaltuutetun toimenpiteet ovat rekisteröidylle ja tietosuojavastaavalle maksuttomia. Jos rekisteröidyn tai tietosuojavastaavan pyynnöt kuitenkin ovat pyyntöjen toistuvuudesta tai muusta syystä ilmeisen kohtuuttomia tai perusteettomia, valtuutettu voi pe-

riä toimenpiteistä maksun tai jättää pyynnön kohteena olevan asian tutkimatta. Maksun määrän perusteista säädetään valtion maksuperustelaissa.

Jos tietosuojavaltuutettu 3 momentissa tarkoitetulla tavalla perii maksun tai jättää asian tutkimatta, sen on tarvittaessa osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

47 §

Tiedonsaantioikeus

Tietosuojavaltuutetulla on oikeus salassapitosäännösten estämättä saada maksutta 22 §:ssä tarkoitettu seloste käsittelytoimista, 19 §:ssä tarkoitetut lokitiedot sekä muut tehtäviensä hoidon kannalta tarpeelliset tiedot.

Tietosuojavaltuutetulla on oikeus saada rekisterinpitäjältä ja henkilötietojen käsittelijältä selvitys seikoista, jotka ovat tarpeen valtuutetun tehtävien hoitamiseksi.

48 §

Oikeus tehdä tarkastuksia

Tietosuojavaltuutettu voi tehdä tarkastuksen rekisterinpitäjän tai henkilötietojen käsittelijän tiloissa, jos tarkastus on tarpeen tämän lain noudattamisen valvomiseksi.

Pysyväisluonteiseen asumiseen käytetyssä tilassa tarkastuksen saa toimittaa vain, jos se on välttämätöntä tarkastuksen kohteena olevien seikkojen selvittämiseksi ja kyseessä olevassa tapauksessa on olemassa perusteltu ja yksilöity syy epäillä henkilötietojen käsittelyä koskevia säännöksiä rikotun tai rikottavan tavalla, josta voi olla seuraamuksena rikoslaissa (39/1889) säädetty vankeusrangaistus.

Tarkastuksessa noudatetaan, mitä hallintolain (434/2003) 39 §:ssä säädetään.

49 §

Virka-apu

Tietosuojavaltuutetulla on oikeus tehtäviensä suorittamiseksi saada pyynnöstä poliisilta virka-apua.

50 §

Asiantuntijoiden käyttö

Tietosuojavaltuutettu voi kuulla ulkopuolisia asiantuntijoita sekä pyytää näiltä lausuntoja.

Tietosuojavaltuutettu voi 48 §:ssä tarkoitetun tarkastuksen yhteydessä käyttää apunaan ulkopuolista asiantuntijaa. Tietosuojavaltuutettu voi nimetä asiantuntijaksi suostumuksensa tehtävään antaneen henkilön, jolla on tietosuojavaltuutetun tehtävän hoitamisen kannalta merkityksellistä asiantuntemusta.

Asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

51 §

Toimenpiteet

Tietosuojavaltuutettu voi tämän lain soveltamisalaan kuuluvassa asiassa:

1) antaa rekisterinpitäjälle ohjausta 21 §:ssä tarkoitetussa ennakkokuulemismenettelyssä;

2) ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle tämän lain väitetystä rikkomisesta;

3) varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet voivat olla tämän lain vastaisia;

4) antaa huomautuksen rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos tämä on käsitellyt henkilötietoja lainvastaisesti;

5) määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat rekisteröidyn tähän lakiin perustuvien oikeuksien käyttöä;

6) määrätä rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle;

7) asettaa väliaikaisen tai pysyvän kiellon tai muun rajoituksen käsittelylle;

8) määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle;

9) määrätä henkilötietojen oikaisemisesta, poistamisesta ja käsittelyn rajoittamisesta sekä niihin liittyvistä muista toimenpiteistä 25 §:n perusteella;

10) määrätä rekisterinpitäjän tai henkilötietojen käsittelijän saattamaan käsittelytoimet tämän lain säännösten mukaisiksi, tarvittaessa määrätyllä tavalla ja kohtuullisen määräajan kuluessa.

52 §

Uhkasakko

Tietosuojavaltuutettu voi asettaa 51 §:n 5–10 kohdassa tarkoitetun päätöksen ja 47 §:ään perustuvaan tietojen luovuttamista koskevan määräyksen tehosteeksi uhkasakon. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990).

Uhkasakkoa ei saa asettaa luonnolliselle henkilölle 1 momentissa tarkoitetun tietojen luovuttamista koskevan määräyksen tehosteeksi, jos henkilöä on aihetta epäillä rikoksesta ja tiedot koskevat rikosepäilyn kohteena olevaa asiaa.

53 §

Tietosuojavaltuutetun kuuleminen

Tietosuojavaltuutettu voi omasta aloitteestaan tai pyynnöstä antaa lausuntoja 1 §:ssä tarkoitettuun henkilötietojen käsittelyyn liittyvistä kysymyksistä.

Tietosuojavaltuutetulle on varattava tilaisuus tulla kuulluksi valmisteltaessa 1 §:ssä tarkoitettua henkilötietojen käsittelyä koskevia lainsäädännöllisiä tai hallinnollisia uudistuksia.

54 §

Keskinäinen avunanto

Tietosuojavaltuutetun on salassapitosäännösten estämättä annettava maksutta toisen EU:n jäsenvaltion vastaavalle valvontaviranomaiselle tämän valvontatehtävässään välttämättä tarvitsemat henkilötiedot sekä muut tarpeelliset tiedot, ja tarvittaessa muutoinkin avustettava tätä valvonnan toteuttamisessa. Tietosuojavaltuutetun on ryhdyttävä muihinkin tarvittaviin toimenpiteisiin tehokkaan keskinäisen yhteistyön varmistamiseksi.

Tietosuojavaltuutetun on vastattava 1 momentissa tarkoitetun valvontaviranomaisen esittämään pyyntöön ilman aiheetonta viivytystä ja joka tapauksessa viimeistään kuukauden kuluttua pyynnön vastaanottamisesta.

9 luku

Oikeusturva

55 §

Lain rikkomista koskeva ilmoitusmenettely

Toimivaltaisella viranomaisella on oltava menettelytavat, joita noudattamalla sille voidaan luottamuksellisesti ilmoittaa tämän lain epäillystä rikkomisesta. Ilmoitusmenettelyn tulee sisältää asianmukaiset ja riittävät toimenpiteet, joilla järjestetään ilmoitusten asianmukainen käsittely. Ilmoitusmenettelyn tulee lisäksi sisältää ohjeet, joilla turvataan ilmoituksen tekijän henkilöllisyyden suoja.

Toimivaltaisen viranomaisen on säilytettävä 1 momentissa tarkoitettua ilmoitusta koskevat tarpeelliset tiedot. Tiedot on poistettava viiden vuoden kuluttua ilmoituksen tekemisestä, jollei tietojen edelleen säilyttäminen ole tarpeen rikostutkinnan, vireillä olevan oikeudenkäynnin, viranomaistutkinnan taikka ilmoituksen tekijän tai ilmoituksen kohteena olevan henkilön oikeuksien turvaamiseksi. Tietojen edelleen säilyttämisen tarpeellisuus on tutkittava viimeistään kolmen vuoden kuluttua edellisestä tarkistamisesta. Tarkistamisesta on tehtävä merkintä.

Kun luonnollinen henkilö on tehnyt toimivaltaiselle viranomaiselle 1 momentissa tarkoitetun ilmoituksen, ilmoittajan henkilöllisyys on pidettävä salassa, jos henkilöllisyyden paljastamisesta voidaan olosuhteiden perusteella arvioida aiheutuvan haittaa ilmoittajalle.

56 §

Oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi

Rekisteröidyllä on oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi (*toimenpidepyyntö*), jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tätä tai muuta henkilötietojen käsittelyä koskevaa lakia. Asian voi rekisteröidyn suostumuksella saattaa tietosuojavaltuutetun käsiteltäväksi myös yleishyödyllinen henkilötietojen suojaa edistävä yhteisö.

57 §

Toimenpidepyynnön käsitteleminen

Tietosuojavaltuutettu voi keskeyttää asian käsittelyn, jos siihen liittyvä asia on vireillä tuomioistuimessa. Valtuutetun on kohtuullisen ajan kuluessa ilmoitettava asian vireillepanijalle asian käsittelemisen etenemisestä, jos asian käsittely viivästyy tarvittavasta lisäselvityksestä tai muusta syystä johtuen.

58 §

Komission päätökset

Jos tietosuojavaltuutettu katsoo sillä vireillä olevassa asiassa tarpeelliseksi selvittää, onko 41 §:n 1 momentin 3 kohdassa tarkoitettu komission päätös tietosuojan tason riittävyydestä rikosasioiden tietosuojadirektiivin mukainen, valtuutettu voi hakemuksella saattaa ennakkoratkaisun pyytämistä koskevan asian Helsingin hallinto-oikeuden ratkaistavaksi.

Hallinto-oikeuden päätökseen saa hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan.

59 §

Muutoksenhaku

Tietosuojavaltuutetun päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen siten kuin hallintolainkäyttölaissa (586/1996) säädetään.

Hallinto-oikeuden päätökseen saa hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan. Myös tietosuojavaltuutettu saa hakea muutosta hallinto-oikeuden päätökseen.

Tietosuojavaltuutetun päätöksessä voidaan määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei valitusviranomainen toisin määrää.

10 luku

Erinäiset säännökset

60 §

Vahingonkorvaus

Rekisterinpitäjä on velvollinen korvaamaan sen taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle tämän lain vastaisesta henkilötietojen käsittelystä.

Muutoin oikeudesta saada korvaus vahingosta säädetään vahingonkorvauslaissa.

61 §

Rangaistussäännökset

Rangaistus tietosuojarikoksesta säädetään rikoslain 38 luvun 9 §:ssä. Rangaistus viestintäsalaisuuden loukkauksesta säädetään mainitun lain 38 luvun 3 §:ssä, törkeästä viestintäsalaisuuden loukkauksesta 4 §:ssä, tietomurrosta 8 §:ssä ja törkeästä tietomurrosta 8 a §:ssä. Rangaistus tämän lain 55 §:n 3 momentissa säädetyn salassapitovelvollisuuden ja 62 §:ssä tarkoitetun vaitiolovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava mainitun lain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta.

62 §

Vaitiolovelvollisuus

Vaitiolovelvollisuudesta ja tietojen hyväksikäyttökiellosta säädetään viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 23 §:ssä.

11 luku

Voimaantulo ja siirtymäsäännökset

63 §

Voimaantulo

Tämä laki tulee voimaan 1 päivänä tammikuuta 2019.

64 §

Siirtymäsäännökset

Ennen 6 päivää toukokuuta 2016 luodut automatisoidut käsittelyjärjestelmät on saatettava 19 §:n mukaisiksi viimeistään 6 päivänä toukokuuta 2023.

Helsingissä 5 päivänä joulukuuta 2018

Tasavallan Presidentti

Sauli Niinistö

Oikeusministeri Antti Häkkänen

JULKAISIJA: OIKEUSMINISTERIÖ ISSN 1455-8904