SELVITYKSIÄ JA OHJEITA
UTREDNINGAR OCH ANVISNINGAR

4
2017

Miten valmistautua EU:n tietosuoja-asetukseen?

TIETOSUOJAVALTUUTETUN TOIMISTO

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

Sarjanimi ja numero 4/2017

Miten valmistautua EU:n tietosuoja-asetukseen?

Oikeusministeriö, Helsinki 2017

Oikeusministeriö

ISBN: 978-952-259-558-4

Helsinki 2017

Kuvailulehti

Julkaisija	Oikeusministeriö Tietosuojavaltuutetun toimisto		27.1.2017
Tekijät	Anu Talus, oikeusministeriö ja Elina Autio, Anna Hänninen, Heljä-Tuulia Pihamaa ja Silja Kantonen, tietosuojavaltuutetun toimisto		
Julkaisun nimi	Miten valmistautua EU:n tietosuoja-asetukseen?		
Julkaisusarjan nimi ja numero	Oikeusministeriön julkaisu 4/2017		
Diaari/hankenumero	OM 3/41/2017	Teema	Selvityksiä ja ohjeita
ISBN painettu	–	ISSN painettu	–
ISBN PDF	978-952-259-558-4	ISSN PDF	1798-7067
URN-osoite	http://urn.fi/URN:ISBN:978-952-259-558-4		
Sivumäärä	40	Kieli	suomi
Asiasanat	henkilötiedot, tietosuoja, henkilötietojen käsittely, yleinen tietosuoja-asetus, GDPR		

Tiivistelmä

Yleinen tietosuoja-asetus on tullut voimaan 24.5.2016 ja sen soveltaminen alkaa 25.5.2018. Henkilötietojen käsittelyn tulee olla yleisen tietosuoja-asetuksen mukaista toukokuussa 2018. Tällä hetkellä sovellettavan henkilötietolain pääperiaatteet säilyvät yleisessä tietosuoja-asetuksessa. Yleisessä tietosuoja-asetuksessa on kuitenkin myös uusia velvoitteita rekisterinpitäjälle ja oikeuksia rekisteröidylle. Tällainen on esimerkiksi rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen.

Oppaassa ”Miten valmistua EU:n tietosuoja-asetukseen” annetaan ohjeita ja neuvoja siitä, miten henkilötietoja tulee käsitellä yleisen tietosuoja-asetuksen mukaisesti. Oppaassa kerrotaan muun muassa henkilötietojen käsittelyn arvioinnista ja oikeusperusteista, tietosuojaperiaatteiden toteuttamisesta sekä tietoturvaloukkauksiin valmistautumisesta.

Opas on suunnattu pääasiassa rekisterinpitäjille, mutta myös henkilötietojen käsittelijä voi tukeutua oppaaseen soveltuvilta osin.

Tietosuojavaltuutetun toimisto ja oikeusministeriö ovat kirjoittaneet oppaan yhteistyössä.

Kustantaja	Oikeusministeriö ja tietosuojavaltuutetun toimisto
Painopaikka ja vuosi	Helsinki 2017
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi,www.oikeusministerio.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Justitieministeriet Dataombudsmannens byrå		27.1.2017
Författare	Anu Talus, justitieministeriet och Elina Autio, Anna Hänninen, Heljä-Tuulia Pihamaa och Silja Kantonen, dataombudsmannens byrå		
Publikationens titel	Förberedelser inför EU:s dataskyddsförordning		
Publikationsseriens namn och nummer	Justitieministeriets publikation 4/2017		
Diarie-/projektnummer	OM 3/41/2017	Tema	Utredningar och anvisningar
ISBN tryckt	–	ISSN tryckt	–
ISBN PDF	978-952-259-558-4	ISSN PDF	1798-7067
URN-adress	http://urn.fi/URN:ISBN:978-952-259-558-4		
Sidantal	40	Språk	finska
Nyckelord	Personuppgifter, dataskydd, behandling av personuppgifter, den allmänna dataskyddsförordningen, GDPR		

Referat

EU:s allmänna dataskyddsförordning trädde i kraft den 24 maj 2016 och börjar tillämpas den 25 maj 2018. Från och med maj 2018 ska personuppgifter behandlas enligt den allmänna dataskyddsförordningen. Huvudprinciperna i den gällande personuppgiftslagen förblir som de är, men dataskyddsförordningen medför dock vissa nya skyldigheter för de registeransvariga och rättigheter för de registrerade. Till dessa hör bl.a. den registrerades rätt att överföra sina uppgifter från ett system till ett annat.

I handboken ”Förberedelser inför EU:s dataskyddsförordning” ges råd och anvisningar om hur personuppgifter ska behandlas enligt den allmänna dataskyddsförordningen. I handboken berättas bl.a. om bedömningen av och de rättsliga grunderna för behandlingen av personuppgifter, på vilket sätt dataskyddsprinciperna ska iakttas samt hur man bereda sig på kränkningar av dataskyddet.

Handboken riktar sig främst till registeransvariga, men i tillämpliga delar även till registerförarna.

Handboken har skrivits i ett samarbete mellan dataombudsmannens byrå och justitieministeriet.

Förläggare	Justitieministeriet och dataombudsmannens byrå
Tryckort och år	Helsingfors 2017
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi, www.oikeusministerio.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Sisältö

JOHDANTO 9

1 Henkilötietojen käsittelyn arviointi 11

2. Tietosuojaperiaatteiden toteuttaminen.....12

2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja.....13

2.2 Osoitusvelvollisuus 14

3. Riskiperusteinen lähestymistapa.....16

4. Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen 17

5. Henkilötietojen käsittelyn oikeusperusteet.....19

6. Henkilötietojen käsittelyn ulkoistaminen 22

7. Rekisteröidyn oikeudet 23

7.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä ...23

7.2 Rekisteröidyn oikeus saada pääsy tietoihin 24

7.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi.....25

7.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta 26

7.5 Oikeus siirtää tiedot järjestelmästä toiseen.....26

7.6 Vastustamisoikeus.....27

7.7 Automatisoidut yksittäispäätökset ja profilointi.....27

8. Organisaation toimiminen useassa EU:n jäsenvaltiossa 29

9. Tietoturva.....31

10. Henkilötietojen tietoturvaloukkauksiin valmistautuminen 32

11. Tietosuojavastaavan nimittäminen 34

12. Tietosuoja-asetuksen tulkinta ja tuleva ohjeistus 36

JOHDANTO

Euroopan unionin tietosuojalainsäädäntö uudistui, kun yleinen tietosuoja-asetus tuli voimaan 24. toukokuuta 2016. Tietosuoja-asetusta sovelletaan kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 alkaen, jolloin henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista.

Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta voidaan vastata teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin. Asetuksen tarkoituksena on myös tukea digitaalitalouden kehitystä sisämarkkinoiden alueella yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset sekä rakentamalla luottamusta.

Tietosuoja-asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Asetuksen velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla: asetuksessa on säädetty henkilötietolakia tiukemmat seuraamukset asetuksen vastaisesta henkilötietojen käsittelystä. Valvontaviranomainen voi esimerkiksi määrätä henkilötietojen käsittelyyn liittyviä korjaavia toimenpiteitä ja hallinnollisia sakkoja.

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita niin rekisterinpitäjiä kuin henkilötietojen käsittelijöitä. Asetuksen soveltamisalaa rajaavat sen aineellista ja alueellista soveltamisalaa koskevat säännökset. Sitä sovelletaan tietyissä asetuksessa määritellyissä tilanteissa myös EU:n ulkopuolelle sijoittautuneisiin organisaatioihin. Asetusta sovelletaan niin yksityisellä kuin julkisella sektorilla riippumatta esimerkiksi henkilötietojen käsittelyn laajuudesta, käsiteltävien henkilötietojen luonteesta tai käytetystä teknologiasta.

Tietosuoja-asetusta sovelletaan automaattiseen henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn, kun henkilötiedot muodostavat rekisterin osan. Asetuksessa henkilötiedon käsite on määritelty vastaavalla tavalla kuin henkilötietolaissa. Asetuk-

sen mukainen henkilötiedon määritelmä on henkilötietolakia yksityiskohtaisempi ja se sisältää konkreettisia esimerkkejä henkilötiedoiksi määriteltävistä tiedoista.

Tietosuojavaltuutetun toimisto ja oikeusministeriö ovat yhteystyössä laatineet tämän ohjeen, jonka tarkoituksena on auttaa henkilötietoja käsitteleviä organisaatioita hahmottamaan, minkälaisten toimenpiteiden toteuttamiseen sen tulee olla valmis siirtymäajan päätyttyä. Ohjeessa on nostettu esille tietosuoja-asetuksen keskeisiä asioita, jotka on otettava huomioon toimintaa suunniteltaessa. Ohje on tarkoitettu ensi sijassa rekisterinpitäjille, mutta myös henkilötietojen käsittelijät voivat soveltuvin osin noudattaa ohjeistuksessa esitettyjä toimintaperiaatteita.

Lue lisää:

Tietosuoja-asetus:

Henkilötiedon määritelmä: 4 artikla kohta 1 ja johdanto-osan kohta 26

Tietosuoja-asetuksen aineellinen soveltamisala: 2 artikla ja johdanto-osan kohdat 14–21

Tietosuoja-asetuksen alueellinen soveltamisala: 3 artikla ja johdanto-osan kohdat 22–25

Tietosuojaviranomaisen tehtävät: artikla 57 ja johdanto-osan kohdat 123 ja 132

Tietosuojaviranomaisen valtuudet: artikla 58 ja johdanto-osan kohta 129

1 Henkilötietojen käsittelyn arviointi

Organisaation on tietosuoja-asetuksen vaikutuksia arvioidessaan hahmotettava kokonaiskuva henkilötietojen käsittelyn nykytilasta. Organisaatio voi esimerkiksi kuvata, mitä henkilötietovarantoja sen hallussa on, miten tietosuojaperiaatteet on otettu huomioon, toimintaan liittyvät henkilötietovirrat, henkilötietojen käsittelyn oikeusperusteet, miten tietoturvasta on huolehdittu ja miten henkilötietojen käsittelyyn liittyvä riskienhallinta on toteutettu. Kartoituksen voi tehdä esimerkiksi laatimalla tietotilinpäätöksen, joka on organisaation sisäisen tarkastelun tuloksena laadittu raportti tietojen käsittelyä koskevista keskeisistä asioista. Tietotilinpäätöstä voidaan käyttää organisaation sisäisenä tietojohtamisen raporttina ja sillä voidaan myös raportoida organisaation sidosryhmille tietojen käsittelyyn liittyvistä asioista.

Kun organisaatio on kartoittanut henkilötietojen käsittelyn nykytilan, sen tulisi selvittää, mitä konkreettisia muutoksia ja toimenpiteitä tietosuoja-asetuksen sääntely sen suorittamalle henkilötietojen käsittelylle tarkoittaa. Tietosuoja-asetus sisältää esimerkiksi täsmennyksiä tietosuojaperiaatteisiin, uusia käsitteitä ja uusia rekisteröityjen oikeuksia. Asetuksen sääntely on osin myös henkilötietolakia yksityiskohtaisempaa. Tietosuoja-asetuksessa rekisterinpitäjään kohdistuvat velvoitteet määräytyvät pääsääntöisesti riskiperusteisen lähestymistavan mukaisesti.

Tietosuoja-asetuksen velvoitteiden edellyttämien toimenpiteiden laatu ja laajuus riippuvat esimerkiksi organisaation käsittelemistä henkilötiedoista, käsittelyyn kohdistuvasta riskistä ja nykyisistä käytännöistä. Erityisesti organisaatioiden johdon on oltava tietoinen lainsäädännössä tapahtuvista muutoksista sekä niiden vaikutuksesta organisaationsa eri toimintoihin.

Työkaluja: Tietotilinpäätöksen tekemiseen ohjeistusta tietosuojavaltuutetun verkkosivuilta www.tietosuoja.fi tietotilinpäätös nimisestä oppaasta.

2. Tietosuojaperiaatteiden toteuttaminen

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ohjaavat rekisterinpitäjää käsittelemään henkilötietoja rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla. Periaatteet vastaavat monilta osin henkilötietolain periaatteita, vaikka asetuksessa osaa näistä periaatteista on täsmennetty. Tietosuoja-periaatteita ovat:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

Rekisterinpitäjän on huolehdittava siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjää koskevan osoitusvelvollisuuden johdosta rekisterinpitäjän on pystyttävä myös osoittamaan, että periaatteita noudatetaan. Rekisterinpitäjän on siis arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa. Periaatteiden noudattamisen osoittaminen edellyttää rekisterinpitäjältä muun muassa henkilötietojen käsittelyn aiempaa tarkempaa suunnittelua ja dokumentointia.

Lue lisää:

Henkilötietojen käsittelyä koskevat periaatteet: 5 artikla ja johdanto-osan kohta 39

Käsittelyn lainmukaisuus: 6 artikla

2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetun tietosuojan periaate edellyttää, että edellä mainitut tietosuojaperiaatteet otetaan tehokkaasti osaksi henkilötietojen käsittelyä sisältäviä toimintoja niiden kaikissa vaiheissa.

Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Rekisterinpitäjän on toteutettava toimenpiteet, jotka varmistavat etenkin sen, että henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Rekisterinpitäjän on käsittelytapoja määrittäessään ja itse käsittelyn yhteydessä toteutettava tietosuojaperiaatteiden täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan suojatoimenpiteitä kuten esimerkiksi henkilöstön koulutusta, henkilöstölle annetut ohjeita ja määräyksiä, salassapitositoumuksia, tilavalvontaa, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta, tietojen anonymisointia, tietojen pseudonymisointia, auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöönottoa.

Rekisterinpitäjän on pääsääntöisesti itse määritettävä asianmukaiset suojatoimet niin, että otetaan huomioon käytettävissä oleva tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet edellyttävät, että tietosuojaa koskevat kysymykset tunnistetaan ja otetaan huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja tai kehitetään tietojärjestelmiä. Tämä on myös kustannustehokkaampi menettelytapa verrattuna siihen, että tehtäisiin muutoksia jo olemassa oleviin toimintoihin ja järjestelmiin. Tietojärjestelmät on jo lähtökohtaisesti rakennettava niin, että ne mahdollistavat rekisterinpitäjän velvoitteiden toteuttamisen, esimerkiksi tarpeettomien tietojen poistamisen ja rekisteröityjen oikeuksien toteuttamisen.

Tietosuoja-asetuksen siirtymäaikana organisaation tulisi varmistaa, että henkilötietoja käsiteltäessä noudatetaan henkilötietolakia. Myös henkilötietolain lähtökohtana on

tietosuojaperiaatteiden sisällyttäminen henkilötietojen käsittelyn osaksi ja käsittelyn toteuttaminen rekisteröityjen oikeuksia suojaavalla tavalla. Sisäänrakennettu ja oletusarvoinen tietosuoja vastaakin pitkälti henkilötietolain käsittelyn suunnittelu- ja huolellisuusvelvoitetta. Periaatteita vastaavia edellytyksiä sisältyy lisäksi esimerkiksi käyttötarkoitussidonnaisuutta, tarpeellisuusvaatimusta ja tietojen suojausta koskeviin henkilötietolain säännöksiin.

2.2 Osoitusvelvollisuus

Osoitusvelvollisuuden toteuttaminen edellyttää uudenlaista suhtautumista tietosuojaa koskeviin kysymyksiin, koska organisaatiolla on oltava kyky osoittaa noudattavansa asetusta henkilötietoja käsitellessä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä. Tämä on keskeinen muutos, koska henkilötietolain aikana on riittänyt, että säännöksiä noudatetaan.

Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia. Kuten sisäänrakennetun ja oletusarvoisen tietosuojanperiaatteiden myös osoitusvelvollisuuden ja rekisterinpitäjän vastuun toteuttamiseksi rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että asetusta noudatetaan. Tällä voidaan tietyissä tilanteissa tarkoittaa myös sitä, että rekisterinpitäjän on pantava täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.

Organisaatiot voivat yhtenä keinona käyttää myös tietosuoja-asetuksen mukaisia tietosuojaa koskevia sertifikaatteja tai käytännesääntöjä sen osoittamiseksi, että rekisterinpitäjälle säädettyjä velvollisuuksia noudatetaan. Organisaatioille myönnettävien sertifikaattien tarkoituksena on antaa rekisteröidyille mahdollisuus arvioida helposti tuotteiden ja palveluiden tietosuojan tasoa. Alakohtaisilla käytännesäännöillä voidaan puolestaan helpottaa asetuksen soveltamista, sillä niissä voidaan ottaa huomioon tietyillä aloilla suoritettavan käsittelyn erityispiirteet ja esimerkiksi erikokoisten organisaatioiden tarpeet henkilötietojen käsittelyyn liittyen.

Tietosuoja-asetuksen mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on pääsääntöisesti ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista, jotta voidaan osoittaa, että ne ovat asetuksen mukaisia. Selosteen on asetuksen mukaan oltava kirjallisessa muodossa ja se on pyydettäessä toimitettava viranomaiselle. Organisaatioiden on siirtymäaikana selvitettävä, koskeeko kyseinen velvollisuus niitä.

KARTOITA TIETOJEN KÄSITTELYN NYKYTILA JA OTA TIETOSUOJA OSAKSI TOIMINTOJEN SUUNNITTELUA JA MALLINNUSTA!

Lue lisää:

Rekisterinpitäjän vastuu: 24 artikla ja johdanto-osan kohdat 74–77

Sisäänrakennettu ja oletusarvoinen tietosuoja: 25 artikla ja johdanto-osan kohta 78

Seloste käsittelytoimista: 30 artikla ja johdanto-osan kohta 82

Käytännesäännöt: 40–41 artiklat ja johdanto-osan kohdat 98–99

Sertifiointi: 42 artikla ja johdanto-osan kohta 100

Työkaluja: Henkilötietojen käsittelyn henkilötietolain mukaisuutta organisaatio voi arvioida tietosuoja ja tietoturvan tee-se-itse -tarkastuksen avulla. Materiaali saatavilla www.tietosuoja.fi

3. Riskiperusteinen lähestymistapa

Tietosuoja-asetuksessa rekisterinpitäjän velvoitteiden määräytymisen osalta on omaksuttu riskiperusteinen lähestymistapa. Riskiperusteinen lähestymistapa tarkoittaa, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Tällä pyritään välttämään matalariskisen toiminnan ylisääntelyä ja suhteuttamaan tarpeelliset toimenpiteet kulloinkin henkilötietojen käsittelyyn liittyvän riskin mukaisesti.

Jotta rekisterinpitäjä voi toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa ja muita asetuksessa säädettyjä velvollisuuksia, on rekisterinpitäjän tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä. Tietosuoja-asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen.

Riski voi olla korkeampi silloin, kun käsitellään esimerkiksi erityisiä henkilötietoryhmiin kuuluvia tietoja, heikossa asemassa olevien (esimerkiksi lasten) tietoja tai kun käsitellään suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää. Riski voi olla korkeampi myös, kun arvioidaan henkilökohtaisia ominaisuuksia – esimerkiksi silloin, kun kyseessä on henkilöprofilointia varten suoritettu analyysi.

ARVIOI HENKILÖTIETOJEN KÄSITTELYYN LIITTYVÄT RISKIT JA TOIMENPITEET RISKIN MINIMOIMISEKSI!

Lue lisää:

Rekisterinpitäjän vastuu: 24 artikla ja johdanto-osan kohdat 74–77

4. Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

Kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on tietosuojaasetuksen mukaan rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi. Riskin tasoa arvioitaessa on otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset edellä selostetun mukaisesti.

Vaikutustenarviointi on tehtävä erityisesti silloin, kun otetaan käyttöön uutta teknologiaa taikka, kun käsitellään laajamittaisesti rikostuomioita tai rikkomuksia taikka erityisiin henkilötietoryhmiin kuuluvia tietoja. Vaikutustenarviointi on tehtävä myös tilanteissa, joissa on kyse järjestelmällisestä ja kattavasta automatisoituun päätöksentekoon perustuvasta arvioinnista sekä tilanteissa, joissa on kyse yleisölle avoimen alueen järjestelmällisestä ja laajamittaisesta valvonnasta.

Vaikutustenarviointi soveltuu laajoihin käsittelytoimiin, joissa on tarkoitus käsitellä huomattavia määriä henkilötietoja tai, jotka voivat vaikuttaa suureen määrään rekisteröityjä. Yhtä arviointia voidaan käyttää samankaltaisiin vastaavia riskejä aiheuttaviin käsittelytoimiin. Rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta, jos sellainen on nimitetty.

Vaikutustenarvioinnissa on tarkasteltava erityisesti suunniteltuja toimenpiteitä sekä suojatoimia ja mekanismeja, joiden avulla voidaan lievittää käsittelyyn kohdistuvaa riskiä ja varmistaa henkilötietojen suoja sekä asetuksen vaatimusten toteutuminen rekisterinpitäjän toiminnassa. Rekisterinpitäjän on aina tarvittaessa varmistettava, että henkilötietojen käsittely tosiasiallisesti tapahtuu vaikutustenarvioinnin mukaisesti.

Vaikutuksenarvioinnin tekeminen on suositeltavaa myös muiden kuin merkittäviä riskejä luovien käsittelytoimien yhteydessä, koska se edesauttaa osoitusvelvollisuuden toteuttamista ja rekisterinpitäjän velvollisuuksien selvittämisessä.

Jos vaikutustenarvioinnin perusteella riskin taso on korkea, eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi, on rekisterinpitäjän kuultava valvontaviranomaista ennen käsittelyn aloittamista. Rekisterinpitäjän on toimitettava valvontaviranomaiselle kuulemista varten rekisterinpitäjää, käsittelyä ja suojatoimia koskevat perustiedot sekä tietosuojaa koskeva vaikutuksenarviointi. Ennakkokuulemisvelvoite tarkoittaa siirtymistä henkilötietolain mukaisesta yleisestä ilmoitusvelvollisuudesta riskiperusteiseen ilmoitusvelvollisuuteen.

Valvontaviranomaisten on laadittava ja julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan tietosuojaa koskeva vaikutustenarviointi. Vastaavasti valvontaviranomainen voi laatia luettelon käsittelytoimien tyypeistä, joiden osalta ei vaadita vaikutustenarviointia. Jos kyse on rajat ylittävästä henkilötietojen käsittelystä, vahvistetaan luettelo tietosuojaneuvostossa.

TEE TARVITTAESSA TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI JA KUULE VALVONTAVIRANOMAISTA!

Lue lisää:

Tietosuojaa koskeva vaikutustenarviointi: 35 artikla ja johdanto-osan kohdat 84, 89–93 ja 95

Ennakkokuuleminen: 36 artikla ja johdanto-osan kohdat 94–96

5. Henkilötietojen käsittelyn oikeusperusteet

Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste. Käsittelyn oikeusperusteista säädetään tietosuoja-asetuksen 6 artiklassa. Erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kielletty. Erityiset henkilötietoryhmän tiedot vastaavat henkilötietolain arkaluonteisia tietotyyppejä eräin muutoksin. Erityisiin henkilötietoryhmiin kuuluvia tietoja voidaan käsitellä, jos 6 artiklassa säädetyn perusteen lisäksi jokin tietosuoja-asetuksen 9 artiklassa säädetty peruste täyttyy.

Rekisterinpitäjän on siirtymäajan aikana selvitettävä, vaikuttaako tietosuoja-asetus sen käyttämiin käsittelyn oikeusperusteisiin. Tämä edellyttää sitä, että rekisterinpitäjä tunnistaa, millä laissa säädetyllä perusteella se käsittelee henkilötietoja. Asetuksen mukaiset käsittelyn oikeusperusteet eroavat joiltakin osin henkilötietolain mukaisiin perusteisiin verrattuna.

Rekisterinpitäjän tai kolmannen osapuolen oikeutettua etua koskeva käsittelyn oikeusperuste sisältyy myös direktiiviin 95/46/EY. Suomen lainsäädäntö on saatettu vastaamaan tätä direktiiviä henkilötietolailla, mutta käsittelyn oikeusperustetta ei ole kirjattu sellaisenaan vaan siitä on säädetty henkilötietolaissa yksityiskohtaisemmin. Esimerkiksi tietosuojalautakunta on voinut myöntää luvan henkilötietojen käsittelyyn rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun edun toteuttamiseksi. Koska tietosuojalautakunnan lupatoimivalta asetuksen myötä poistuu, rekisterinpitäjän on arvioitava jatkossa, edellyttääkö joku hänen tai kolmannen osapuolen oikeutettu etu henkilötietojen käsittelyä.

Direktiivin oikeutettua etua koskeva käsittelyperuste on mahdollistanut myös muun muassa asiakas- tai palvelussuhdetta koskevan oikeusperusteen sisällyttämisen henkilötietolakiin. Tätä vastaava ajatus on kirjattu myös tietosuoja-asetukseen, jonka mukaan oikeutettu etu voi olla olemassa esimerkiksi silloin, kun rekisteröidyn ja rekis-

terinpitäjän välillä on merkityksellinen ja asianmukainen suhde − rekisteröity on esimerkiksi rekisterinpitäjän asiakas tai tämän palveluksessa.

Henkilötietojen käsittely ei kuitenkaan ole oikeutetusta edusta huolimatta sallittua, jos henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet ne syrjäyttävät. Näin on erityisesti silloin, kun rekisteröity on lapsi. Myös sen arvioiminen, syrjäyttävätkö rekisteröidyn edut tai perusoikeudet ja -vapaudet rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun, jää rekisterinpitäjän itsensä arvioitavaksi. Valvontaviranomainen tai tuomioistuin arvioi viime kädessä henkilötietojen käsittelyn lainmukaisuuden myös käsittelyn oikeusperusteen osalta.

Jako suostumukseen henkilötietojen käsittelyperusteena ja nimenomaiseen suostumukseen erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyn oikeusperusteena säilyy asetuksen soveltamiseen siirryttäessä. Suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen. Erityisten henkilötietoryhmien kohdalla suostumuksen on oltava nimenomainen.

Jos henkilötietoja käsitellään suostumuksen perusteella, on kiinnitettävä huomiota siihen, miten suostumus pyydetään. Asetuksen mukaan suostumus on annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, sähköisellä tai suullisella lausumalla. Lausumasta on käytävä ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn.

Suostumuksen on katettava kaikki käsittelytarkoitukset. Suostumusta ei voi antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jonkin toimen toteuttamatta. Jos rekisteröidyn on annettava suostumuksensa sähköisen pyynnön perusteella, pyynnön on oltava selkeä ja tiiviisti esitetty, eikä se saa tarpeettomasti häiritä sen palvelun käyttöä, jota varten se annetaan. Asetuksessa suostumukselle on annettu henkilötietolakia tarkempia kriteereitä, ja lisäksi on huomioitava, että rekisterinpitäjää koskeva osoitusvelvollisuus koskee myös suostumuksen olemassaoloa.

Lapsille palveluita tarjoavien rekisterinpitäjien on huomioitava, että tietosuoja-asetus antaa henkilötietolaista poiketen erityistä suojaa lapsien henkilötiedoille. Asetuksen mukaan lapsen henkilötietojen käsittely suostumuksen perusteella suoraan lapselle tarjottavien tietoyhteiskunnan palvelujen tarjoamisen yhteydessä edellyttää vanhempainvastuunkantajan suostumusta tai valtuutusta. Asetuksessa lapseksi määritellään alle 16-vuotiaat. Tätä alhaisempi ikäraja, joka voi olla vähintään 13 vuotta, voidaan määritellä kansallisella lainsäädännöllä.

SELVITÄ, MILLÄ PERUSTEELLA KÄSITTELET HENKILÖTIETOJA!

Lue lisää:

Käsittelyn lainmukaisuus: artikla 6 sekä johdanto-osan kohdat 40, 41 ja 44–50

Suostumuksen edellytykset: artikla 7 sekä johdanto-osan kohdat 32, 33, 42 ja 43

Tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot: 8 artikla ja johdanto-osan kohta 38

Erityisiä henkilötietoryhmiä koskeva käsittely: 9 artikla ja johdanto-osan kohdat 51–56

6. Henkilötietojen käsittelyn ulkoistaminen

Osana henkilötietojen käsittelyä koskevan toiminnan arviointia on myös huomioitava, ulkoistetaanko tietojen käsittelyyn liittyviä tehtäviä henkilötietojen käsittelijälle. Tällä tarkoitetaan esimerkiksi tietojen säilytys- ja analysointipalveluiden ostamista toiselta organisaatiolta. Rekisterinpitäjän on tunnistettava tietosuoja-asetuksen vaatimukset henkilötietojen käsittelyn ulkoistamiselle, sillä tietosuoja-asetuksessa henkilötietojen käsittelijän roolia ja velvoitteita on terävöitetty henkilötietolakiin nähden.

Henkilötietojen käsittelijän on annettava riittävät takeet siitä, että sen suorittama henkilötietojen käsittely täyttää tietosuoja-asetuksen vaatimukset. Henkilötietojen käsittelijä voi osittain osoittaa riittävien takeiden olemassaolon noudattamalla asetuksen mukaisia hyväksyttyjä käytännesääntöjä tai sertifiointimekanismeja.

Tietosuoja-asetuksessa säädetään myös muun muassa siitä, mistä seikoista rekisterinpitäjän ja toimeksisaajan välisissä toimeksiantosopimuksissa on erityisesti sovittava. Siirtymäaikana on syytä tarkastaa henkilötietojen käsittelyyn liittyvät sopimukset niin, että ne vastaavat asetuksessa säädettyjä ehtoja.

HENKILÖTIETOJEN KÄSITTELIJÄN ROOLI; KÄYTÄTKÖ TOISEN ORGANISAATION TIETOJENKÄSITTELYPALVELUITA?

Lue lisää:

Henkilötietojen käsittelijä: 28 artikla ja johdanto-osan kohta 81

7. Rekisteröidyn oikeudet

Rekisterinpitäjän yhtenä velvollisuutena on toteuttaa rekisteröidyn oikeuksia. Rekisteröidyn oikeudet on otettava huomioon henkilötietojen käsittelyyn liittyvien prosessien ja tietojärjestelmien suunnittelussa. Organisaatioiden on varmistuttava siitä, että nykyiset prosessit ja tietojärjestelmät taipuvat tietosuoja-asetuksen tuomiin muutoksiin myös rekisteröityjen oikeuksien osalta.

Rekisteröidyn oikeudet vastaavat suurilta osin henkilötietolain mukaisia oikeuksia, mutta tietosuoja-asetuksessa oikeuksien toteuttamiseen liittyvä sääntely on yksityiskohtaisempaa. Asetuksessa on säädetty myös uusista rekisteröidyn oikeuksista. Oikeuksien toteuttamiseen liittyvät prosessit muuttuvat myös jonkin verran asetuksen myötä.

Henkilötietojen käsittelyyn liittyviä toimintoja suunniteltaessa on myös huomioitava, että käsittelyn oikeusperuste vaikuttaa jonkin verran siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeus siirtää tiedot järjestelmästä toiseen ja vastustamisoikeus liittyvät vain osaan käsittelyperusteista. Osana henkilötietojen käsittelytoimintojen suunnittelua rekisterinpitäjän tulisi selvittää, mitä rekisteröidyn oikeuksia käytössä oleviin käsittelyn perusteisiin liittyy ja miten rekisteröityjen oikeuksien toteuttaminen käytännössä toteutetaan.

7.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

Tietosuoja-asetuksessa korostetaan henkilötietojen käsittelyn avoimuutta ja annetaan henkilötietolakia yksityiskohtaisempia määräyksiä rekisterinpitäjän informointivelvollisuuden ja rekisteröidyn oikeuksien toteuttamisesta.

Rekisterinpitäjän on toimitettava henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Asetus asettaa määräaikoja informoinnille ja rekisteröidyn pyynnön perusteella toteutettaville toimenpiteille. Asetuksen mukaan tieto toimenpiteistä, joihin rekisteröidyn pyynnön johdosta on ryhdytty, tulee antaa ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa.

Kuukauden määräaika pätee myös rekisterinpitäjän velvollisuuteen ilmoittaa rekisteröidylle syy siihen, miksi rekisterinpitäjä ei aio toteuttaa rekisteröidyn pyytämiä toimenpiteitä. Kieltäytyessään suorittamasta rekisteröidyn pyytämää toimea, rekisterinpitäjän on kerrottava rekisteröidylle tämän käytettävissä olevista oikeussuojakeinoista, kuten oikeudesta tehdä valitus valvontaviranomaiselle. Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän toimet rekisterinpitäjän oikeuksien toteuttamiseksi ovat lähtökohtaisesti maksuttomia.

Rekisteröidylle asetuksen mukaan annettavat tiedot sisältyvät suurelta osin jo henkilötietolain mukaiseen informointivelvoitteeseen, mutta asetuksen mukainen informointi on tietosisällöllisesti henkilötietolain mukaista informointia laajempi ja yksityiskohtaisempi. Asetuksessa informoinnista on säädetty erikseen siitä, miten rekisteröityä tulee informoida tilanteissa, joissa henkilötiedot kerätään suoraan rekisteröidyltä ja toisaalta tilanteissa, joissa henkilötiedot kerätään muualta kuin rekisteröidyltä itseltään. Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle artikloissa säädetyt tiedot.

Asetuksessa määritellään henkilötietolakia tarkempi määräaika henkilötietojen käsittelyä koskevan tiedon antamiselle, silloin kun kerättäviä henkilötietoja ei ole saatu rekisteröidyltä. Tieto henkilötietojen käsittelystä on toimitettava kohtuullisen ajan kuluttua, mutta viimeistään kuukauden kuluessa henkilötietojen saamisesta. Mikäli tietoja käytetään viestintään kyseisen rekisteröidyn kanssa, tiedot on toimitettava viimeistään silloin, kun näitä tietoja luovutetaan ensimmäisen kerran. Jo henkilötietolaissa säädetty velvollisuus ilmoittaa käsittelystä viimeistään silloin, kun tietoja luovutetaan ensimmäisen kerran, pysyy voimassa.

7.2 Rekisteröidyn oikeus saada pääsy tietoihin

Asetuksessa säädetään rekisteröidyn oikeudesta saada pääsy tietoihin, jota koskeva sääntely on hieman yksityiskohtaisempaa henkilötietolain mukaiseen tarkastusoikeuteen nähden. Asetuksen mukaisen oikeuden nojalla rekisteröidyllä on oikeus saada

jäljennös häntä koskevista henkilötiedoista. Toisin kuin henkilötietolaissa, tietosuoja-asetuksessa ei säädetä määrämuotoa pyynnön esittämiselle. Jos rekisterinpitäjällä on perusteltu syy epäillä pyynnön tehneen luonnollisen henkilön henkilöllisyyttä, rekisterinpitäjä voi kuitenkin pyytää toimittamaan lisätiedot, jotka ovat tarpeen rekisteröidyn henkilöllisyyden vahvistamiseksi.

Jos rekisteröity esittää oikeutta koskevan pyynnön sähköisesti, rekisterinpitäjän on toimitettava tiedot yleisesti käytetyssä sähköisessä muodossa, ellei rekisteröity toisin pyydä. Pyyntöjen toteuttamisen lähtökohtana on maksuttomuus, mutta rekisterinpitäjä voi tietyin edellytyksin periä pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset tai kieltäytyä suorittamista pyydettyä toimea, mikäli rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia. Tällöin rekisterinpitäjän on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

Tietosuoja-asetuksessa aikaraja rekisteröidyn esittämään pyyntöön reagoimiselle on yksi kuukausi. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Rekisterinpitäjän on ilmoitettava rekisteröidylle mahdollisesta määräajan jatkamisesta kuukauden kuluessa pyynnön vastaanottamisesta sekä kerrottava viivästymisen syyt.

7.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Tietosuoja-asetus takaa rekisteröidylle tietyin poikkeuksin oikeuden tietojen oikaisemiseen sekä oikeuden tietojen poistamiseen eli niin kutsutun oikeuden tulla unohdetuksi. Vastaavat oikeudet sisältyvät myös henkilötietolakiin, vaikka oikeutta tulla unohdetuksi ei ole kirjattu lakiin nimenomaisesti.

Asetuksessa säädetään rekisterinpitäjälle velvollisuudesta ilmoittaa henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt poistamaan henkilötietoihin liittyvät linkit tai näiden henkilötietojen jäljennökset tai kopiot. Myös henkilötietolakiin sisältyy velvollisuus ilmoittaa tiedon korjaamisesta sille, jolle rekisterinpitäjä on luovuttanut tai jolta rekisterinpitäjä on saanut henkilötiedon.

7.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

Tietosuoja-asetuksessa säädetään myös oikeudesta käsittelyn rajoittamiseen. Rekisteröidyllä on asetuksessa luetelluissa neljässä eri tilanteessa oikeus saada aktiivinen käsittely rajoitetuksi. Oikeus on olemassa muun muassa silloin, kun rekisteröity esittää henkilötietojen oikaisua tai poistoa koskevan pyynnön ja näin ollen kiistää henkilötietojen paikkaansa pitävyyden.

Henkilötietojen käsittelyn rajoittamista koskevia menetelmiä voivat olla esimerkiksi valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estäminen valittuihin henkilötietoihin. Käsittelyn rajoittaminen on ilmaistava järjestelmässä selkeästi ja varmistettava teknisesti niin, etteivät henkilötiedot enää myöhemmin joudu käsittelytoimenpiteiden kohteeksi.

Rekisterinpitäjä saa edelleen säilyttää tietoja, muttei muutoin käsitellä niitä ilman rekisteröidyn suostumusta. Rekisterinpitäjä saa käsitellä rekisteröidyn henkilötietoja myös esimerkiksi oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai tärkeää jäsenvaltion etua koskevista syistä. Ennen kuin käsittelyn rajoitus poistetaan, rekisterinpitäjän on ilmoitettava siitä rekisteröidylle.

7.5 Oikeus siirtää tiedot järjestelmästä toiseen

Asetuksen mukaan rekisteröidyllä on oikeus siirtää rekisterinpitäjälle toimittamansa häntä koskevat henkilötiedot rekisterinpitäjältä toiselle sen rekisterinpitäjän estämättä, jolle tiedot on toimitettu. Tiedot on voitava siirtää jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Rekisteröidyllä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, mikäli se on teknisesti mahdollista.

Rekisteröidyllä on oikeus siirtoon vain silloin, jos käsittely perustuu suostumukseen tai sopimukseen, ja jos käsittely suoritetaan automaattisesti. Rekisteröidyn oikeutta siirtää tiedot järjestelmästä toiseen ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Rekisteröidyn oikeus ei saa myöskään vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin.

Rekisterinpitäjien kannattaa hyvissä ajoin selvittää, koskeeko kyseinen oikeus sen käsittelemiä henkilötietoryhmiä ja vastaako käytössä oleva tietojenantotapa kyseisen oikeuden asettamia vaatimuksia.

Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä WP 29 on antanut ohjausta oikeudesta siirtää tiedot järjestelmästä toiseen. Ohjaus on saatavilla englanniksi osoitteessa:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

7.6 Vastustamisoikeus

Asetus takaa rekisteröidylle oikeuden vastustaa henkilötietojensa käsittelyä tietyissä tilanteissa. Vastustamisoikeus liittyy vain osaan käsittelyperusteista. Se kattaa käsittelyn, joka perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttöön sekä rekisterinpitäjän tai kolmannen oikeutetun edun toteuttamiseen. Lisäksi vastustamisoikeus koskee käsittelyä suoramarkkinointia varten sekä tietyin edellytyksin myös käsittelyä tieteellistä, historiallista tai tilastollista tutkimusta varten, tästä oikeudesta voidaan kuitenkin säätää poikkeuksia kansallisella lailla. Rekisteröidyn käyttäessä vastustamisoikeuttaan rekisterinpitäjä ei lähtökohtaisesti saa enää käsitellä henkilötietoja. Asetuksessa määritellään kuitenkin edellytykset käsittelykiellosta poikkeamiseen.

Rekisterinpitäjä on velvollinen informoimaan rekisteröityä vastustamisoikeudesta viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran. Tieto rekisteröidyn oikeudesta on esitettävä selkeästi ja muusta tiedotuksesta erillään. Tietoyhteiskunnan palvelujen käyttämisen yhteydessä rekisteröidyn on voitava käyttää vastustamisoikeuttaan automaattisesti teknisiä ominaisuuksia hyödyntäen.

7.7 Automatisoidut yksittäispäätökset ja profilointi

Kuten henkilötietolaki, myös tietosuoja-asetus kieltää, tiettyjä poikkeustilanteita lukuun ottamatta, sellaisten automatisoitujen päätösten tekemisen, joilla on rekisteröityjä koskevia oikeusvaikutuksia tai jotka vaikuttavat häneen vastaavalla tavalla merkittävästi.

Asetus velvoittaa rekisterinpitäjän toteuttamaan toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. Asetuksen mukaan rekisteröidyllä on oikeus vähintään vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö, esittämään kantansa asiassa ja riitauttamaan tehdyn päätöksen. Automatisoidut päätökset ja profilointi eivät saa perustua erityisiin henkilötietoryhmiin. Erityisiin henkilötietoryhmiin perustuvat automatisoidut päätökset ovat kuitenkin sallittuja tietyissä poikkeustilanteissa.

MITÄ REKISTERÖIDYN OIKEUKSIA LIITTYY TOIMINTAASI JA, MITEN TOTEUTAT REKISTERÖIDYN OIKEUKSIA?

Lue lisää:

Rekisteröidyn oikeudet: artiklat 12–22 ja johdanto-osan kohdat 58–72

8. Organisaation toimiminen useassa EU:n jäsenvaltiossa

Tietosuoja-asetuksen myötä rekisterinpitäjän ei tarvitse asioida kuin yhden jäsenvaltion valvontaviranomaisen kanssa. Jos organisaation toiminta liittyy useaan EU:n jäsenvaltioon, organisaation täytyy selvittää, minkä jäsenvaltion valvontaviranomaisen kanssa se asetuksen mukaan asioi. Toimivaltainen valvontaviranomainen määräytyy one-stop-shop-mekanismin eli yhden luukun periaatteen mukaisesti rekisterinpitäjän tai henkilötietojen käsittelijän ainoan toimipaikan tai päätoimipaikan mukaan.

Toimivaltaista valvontaviranomaista kutsutaan johtavaksi valvontaviranomaiseksi ja se toimii rekisterinpitäjän tai henkilötietojen käsittelijän ainoana yhteyspisteenä kaikissa henkilötietojen käsittelyyn liittyvissä kysymyksissä. Myös useampaan eri jäsenvaltioon sijoittautunut organisaatio voi jatkossa olla tekemisissä vain yhden valvontaviranomaisen kanssa.

Päätoimipaikan määrittyminen riippuu esimerkiksi siitä, millainen organisaation rakenne on ja miten sen henkilötietojen käsittelyyn liittyvät toiminnot on järjestetty. Lisäksi tulee huomioida, että asetuksessa annettu päätoimipaikan määritelmä eroaa rekisterinpitäjän ja henkilötietojen käsittelijän välillä.

Direktiivin 95/46/EY 29 artiklan nojalla perustettu EU:n tietosuojatyöryhmä WP 29 on antanut ohjausta johtavan valvontaviranomaisen määräytymisestä. Ohjaus saatavilla englanniksi osoitteessa:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

TOIMIIKO ORGANISAATIOSI USEAN JÄSENVALTION ALUEELLA? KUKA ON JOHTAVA VALVONTAVIRANOMAINEN?

Lue lisää:

Päätoimipaikan määritelmä: artikla 4 (kohta 16) ja johdanto-osan kohta 36

9. Tietoturva

Siirtymäaikana rekisterinpitäjän tai henkilötietojen käsittelijän on selvitettävä, vastaavatko sen tietojen suojaamista koskevat käytännöt ja toimenpiteet tietosuojaasetuksen riskiperusteista ja osittain henkilötietolakia yksityiskohtaisempaa sääntelyä.

Rekisterinpitäjän tai henkilötietojen käsittelijän on arvioitava käsittelyyn liittyvät riskit ja toimittava näiden riskien lieventämiseksi. Toimenpiteiden avulla varmistetaan asianmukainen turvallisuustaso, kun otetaan huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen.

Tietojen suojaamisesta on huolehdittava kaikissa käsittelyn vaiheissa alkaen tietojen keräämisestä ja päättyen tietojen tuhoamiseen. Käsittelyn turvallisuus edellyttää esimerkiksi kykyä taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kykyä palauttaa tietojen saatavuus ja pääsy tietoihin nopeasti fyysisen tai teknisen vian sattuessa. Tietojen suojaaminen edellyttää myös henkilötietojen käsittelyn seuraamista ja valvontaa.

ARVIOI ASIANMUKAISET SUOJATOIMENPITEET RISKIPERUSTEISTI, SUOJAA KOKO HENKILÖTIEDON ELINKAARI

Lue lisää:

Käsittelyn turvallisuus: 32 artikla ja johdanto-osan kohta 83

10. Henkilötietojen tietoturvaloukkauksiin valmistautuminen

Uutena asiana tietosuoja-asetuksessa säädetään rekisterinpitäjän velvollisuudesta ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Rekisterinpitäjän on tehtävä loukkausta koskeva ilmoitus valvontaviranomaiselle mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta. Rekisterinpitäjä voi jättää tietoturvaloukkausta koskevan ilmoituksen tekemättä ainoastaan, mikäli loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Henkilötietojen käsittelijän on puolestaan ilmoitettava tietoturvaloukkauksista rekisterinpitäjälle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan.

Rekisterinpitäjä on velvollinen ilmoittamaan henkilötietojen tietoturvaloukkauksesta myös rekisteröidyille, jos loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Rekisteröidyille tehtävässä ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä muun muassa henkilötietojen tietoturvaloukkauksen luonne ja tietoturvaloukkauksen todennäköiset seuraukset. Rekisterinpitäjän on tehtävä tällainen ilmoitus ilman aiheetonta viivytystä. Asetus kuitenkin sallii ilmoituksen tekemättä jättämisen tiettyjen edellytysten täyttyessä.

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset ja loukkaukseen liittyvät seikat, loukkauksen vaikutukset ja toteutetut korjaavat toimet. Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa, että rekisterinpitäjä on noudattanut ilmoitusvelvollisuuttaan.

Osana henkilötietojen käsittelyn suunnittelua tulisi suunnitella prosessit myös mahdollisten tietoturvaloukkausten varalle, jotta tietoturvaloukkaukseen liittyvien ilmoitusvelvollisuuksien täyttäminen olisi mahdollista. Organisaatioissa tulisi suunnitella miten mahdollinen tietoturvaloukkaus tunnistetaan, ilmoitetaan, selvitetään ja dokumentoidaan, jotta organisaatio pystyy toimimaan tehokkaasti vahingon minimoimiseksi ja toimintakykyisyyden palauttamiseksi. Eri tilanteita varten tulisi laatia toimintaohjelmat, minkä lisäksi tulisi huolehtia henkilöstön osaamisesta kriisitilanteessa.

VALMISTAUDU ILMOITTAMAAN TIETOTURVALOUKKAUKSISTA!

Lue lisää:

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle: 33 artikla sekä johdanto-osan kohdat 85, 87 ja 88

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle: 34 artikla ja johdanto-osan kohdat 86–88

11. Tietosuojavastaavan nimittäminen

Rekisterinpitäjien ja henkilötietojen käsittelijöiden on varmistuttava siitä, onko organisaatioon asetuksen mukaan nimettävä tietosuojavastaava. Tietosuojavastaavan tehtävänä on muun muassa seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Tietosuojavastaavan tehtävänä on myös toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tästä johtuen organisaation on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle. Tietosuojavastaava ei kuitenkaan ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta vaan vastuu kuuluu edelleen organisaation johdolle.

Velvollisuus tietosuojavastaavan nimittämiseen asetuksen mukaan tulee kyseeseen kun

- on kyse julkisen sektorin toimijasta, joka ei ole tuomioistuin
- organisaation ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- organisaation ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Tietosuoja-asetus sisältää yksityiskohtaiset säännökset tietosuojavastaavan asemasta ja tehtävistä. Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi tietyin edellytyksin nimittää vain yhden tietosuojavastaavan. Nimitettäessä tietosuojavastaavaa tulee ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä. Tietosuojavastaavan on oltava riippumaton eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä.

Tällä hetkellä sosiaali- ja terveydenhuollon palveluita tarjoavilla sekä apteekeilla on velvollisuus nimittää tietosuojavastaava voimassa olevan kansallisen lainsäädännön nojalla.

Tietosuojavastaava voidaan nimittää, vaikkei tietosuoja-asetus tähän nimenomaisesti velvoita. Niissä tilanteissa, joissa tietosuojavastaavan nimittäminen ei ole nimenomaisesti velvollisuus, on organisaatiossa kuitenkin syytä määritellä henkilö, jonka tehtävänä on tietosuojaa koskevien asioiden huomioon ottaminen organisaation toiminnassa ja joka voi toimia yhteyshenkilönä rekisteröidyn oikeuksiin ja viranomaisvalvontaan liittyvissä kysymyksissä.

Organisaation on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle.

Tietosuojadirektiivin 95/46/EY 29 artiklan nojalla perustettu EU:n tietosuojatyöryhmä WP 29 on antanut ohjausta tietosuojavastaavista. Ohjaus saatavilla englanniksi osoitteessa: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

TULEEKO ORGANISAATION NIMITTÄÄ TIETOSUOJAVASTAAVA?

Lue lisää:

Tietosuojavastaan nimittäminen: 37 artikla ja johdanto-osan kohta 97

Tietosuojavastaavan asema: 38 artikla ja johdanto-osan kohta 97

Tietosuojavastaavan tehtävät: 39 artikla

12. Tietosuoja-asetuksen tulkinta ja tuleva ohjeistus

Tietosuoja-asetuksen yhtenä keskeisenä tarkoituksena on harmonisoida EU:n jäsenvaltioiden tietosuojaa koskevat säännökset. Jotta harmonisointitavoite toteutuu, asetuksen tulkinnan on oltava mahdollisimman yhdenmukaista jokaisessa jäsenvaltiossa.

Moni asia täsmentyy vasta siirtymäajan kuluessa, joten on tärkeää seurata tiedottamista. EU:n tietosuojatyöryhmä WP 29 laatii siirtymäaikana ohjeistusta tietosuoja-asetuksen tulkinnasta. Lisäksi siirtymäaikana toteutetaan asetuksen edellyttämiä muutoksia kansalliseen lainsäädäntöön.

Tietosuoja-asetuksen tulkinta tarkentuu oikeuskäytännön kautta. Esimerkiksi henkilötietolakia ja henkilötietodirektiiviä koskevia tulkintalinjauksia tehdään yhä yli 20 vuotta direktiivin hyväksymisen jälkeen. Tulkintalinjaukset koskevat jopa keskeisiä käsitteitä.

Asetuksen tavoitteena on muun muassa varmistaa henkilötietojen käsittelyä koskevien sääntöjen johdonmukainen ja yhtenäinen soveltaminen kaikkialla EU:ssa. Tietosuojatyöryhmän tulkintaohjeet ovat keskeisessä roolissa asetusta tulkittaessa. Ensimmäiset rekisterinpitäjille ja henkilötietojen käsittelijöille tehtävät ohjeet keskittyvät:

- oikeuteen siirtää tiedot järjestelmästä toiseen
- korkean riskin käsitteeseen ja tietosuojaa koskevaan vaikutustenarviointiin
- sertifiointiin
- tietosuojavastaavaan

Siirtyminen asetuksen soveltamiseen edellyttää myös henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistamista. Tietosuoja-asetus jättää myös tietyissä kysymyksissä jäsenvaltioiden lainsäädännölle kansallista liikkumavaraa, jonka nojalla annettavalla lainsäädännöllä on mahdollista tarkentaa asetuksen säännöksiä ja jossain määrin myös poiketa asetuksen velvoitteista. Kansallista lainsäädäntöä ja liikku-

mavaran käyttöä arvioidaan oikeusministeriön asettamassa työryhmässä, jonka tulee saada mietintönsä lainsäädännön muutosehdotuksista valmiiksi 31.5.2017 mennessä.

Tietosuojavaltuutetun toimisto julkaisee tietosuoja-asetukseen liittyviä ohjeita verkkosivuillaan.

Lue lisää:

Tietosuojatyöryhmä WP 29:n kannanottoja ja suosituksia

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

ISSN 1798-7067
ISBN 978-952-259-558-4 (PDF)

Oikeusministeriö
PL 25
00023 Valtioneuvosto
www.oikeusministerio.fi

Justitieministeriet
PB 25
00023 Statsrådet
www.oikeusministerio.fi