Kuntaliitto
Kommunförbundet

Ida Sulin

**Yleiskirje**

14/2017

29.5.2017

Kunnan- ja kaupunginhallituksille
Kuntayhtymien hallituksille

**Yleinen tietosuoja-asetus**

Euroopan unionin yleinen tietosuoja-asetus on tullut voimaan toukokuussa 2016 ja sitä sovelletaan kansallisesti 25.5.2018 alkaen. Tässä yleiskirjeessä käsitellään tietosuoja-asetuksen vaatimuksia rekisterinpitäjän, henkilötietojen käsittelijän ja rekisteröidyn näkökulmasta. Yleiskirjeessä käsitellään myös asetuksen toiminnallisia vaatimuksia ja vaikutuksia sopimuksiin.

Tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn sekä julkisella että yksityisellä sektorilla. Asetuksen tavoitteena on varmistaa, että ihmisten oikeus henkilötietojen suojaan ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana.

**Lisätiedot:**

Palvelusähköposti: hallintolakimiehet@kuntaliitto.fi

Ida Sulin, lakimies, puh. 050 563 3023
Tuula Seppo, erityisasiantuntija, puh. 050 428 8255

# Tietosuoja-asetus

Euroopan unionin yleinen tietosuoja-asetus (EU 679/2016) on tullut voimaan toukokuussa 2016 ja sitä sovelletaan kansallisesti 25.5.2018 alkaen. Asetusta sovelletaan henkilötietojen käsittelyyn sekä julkisella että yksityisellä sektorilla. Asetus korvaa vuoden 1995 henkilötietodirektiivin sekä sen kansallisesti täytäntöön panemiseksi annetun henkilötietolain (523/1999). Asetuksen rinnalle säädetään uusi tietosuojalaki.

Asetuksen tavoitteena on varmistaa, että ihmisten oikeus henkilötietojen suojaan ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana. Sääntely pyrkii vastaamaan teknologian nopean kehityksen haasteisiin ja vahvistamaan ihmisten oikeutta valvoa henkilötietojaan. Tavoitteena on myös vahvistaa säännöt henkilötietojen vapaalle liikkuvuudella EU:n sisällä.

Asetus tuo sekä rekisterinpitäjille että henkilötietojen käsittelijöille uusia tehtäviä ja velvollisuuksia. Asetus pitää myös sisällään uusia oikeuksia rekisteröidyille. Asetus ottaa kantaa henkilötietojen lainmukaiseen käsittelyyn ja kertoo milloin, miten ja kenen toimesta henkilötietoja saa käsitellä.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus): http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=en

## Soveltamisala ja määritelmät

Asetuksen soveltamisala (artiklat 2 ja 3)

Tietosuoja-asetusta sovelletaan automaattiseen henkilötietojen käsittelyyn. Asetusta sovelletaan myös muussa kuin automaattisessa muodossa tapahtuvaan henkilötietojen käsittelyyn silloin, kun käsiteltävät henkilötiedot muodostavat rekisterin osan.

Tietosuoja-asetusta sovelletaan aina kun henkilötietoja käsitellään organisaation EU:n alueella sijaitsevan toimipaikan toiminnan yhteydessä, riippumatta siitä, suoritetaanko itse käsittely unionin alueella. Lisäksi asetusta sovelletaan tietyissä tilanteissa myös EU:n ulkopuolelle sijoittuneisiin organisaatioihin. Asetusta sovelletaan esimerkiksi unionissa olevia henkilöitä koskevien tietojen käsittelyyn, jos käsittely liittyy tavaroiden tai palveluiden tarjoamiseen näille henkilöille tai näiden henkilöiden käyttäytymisen.

Asetusta ei sovelleta luonnollisen henkilön suorittamaan henkilötietojen käsittelyyn toiminnassa, joka on yksinomaan henkilökohtaista tai kotitaloutta koskevaa ja joka ei ole sidoksissa mihinkään ammatilliseen tai kaupalliseen toimintaan. Henkilökohtaista tai kotitaloutta koskevaa toimintaa voi olla esimerkiksi osoitteiston pitäminen tai sosiaalinen verkostoituminen, joita harjoitetaan tällaisen henkilökohtaisen tai kotitaloutta koskevan toiminnan yhteydessä.

Tietosuoja-asetusta ei sovelleta kansallista turvallisuutta koskeviin toimiin. Asetus ei koske henkilötietojen käsittelyä EU:n jäsenvaltioissa niiden toteuttaessa unionin yhteiseen ulko- ja turvallisuuspolitiikkaan liittyvää toimia. Lisäksi, asetusta ei sovelleta henkilötietojen käsittelyyn, jota toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten. Näiden käsittelytarkoitusten osalta sääntely perustuu EU:n antamaan direktiiviin (Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 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).

Keskeiset määritelmät (artikla 4)

Tietosuoja-asetuksen henkilötiedon määritelmä on vanhan henkilötietolain määritelmää yksityiskohtaisempi ja asetuksen määritelmään sisältyy esimerkkejä henkilötiedoksi määriteltävistä tiedoista.

Asetuksen mukaan henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötieto voi määritelmän mukaan olla esimerkiksi paikkatieto, joka kertoo jotakin tietystä henkilöstä; kuva, joka yhdistettynä esimerkiksi osoitetietoihin kertoo jotakin tietystä henkilöstä tai tämän elinolosuhteista; tai IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään; tai käyttäjätunnus.

Henkilötiedon käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, esimerkiksi tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Henkilörekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. Esimerkiksi jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

**Henkilötietojen lainmukainen käsittely ja tietosuojaperiaatteet**

Henkilötietojen lainmukainen käsittely (artikla 6)

Rekisterinpitäjä ja käsittelijä saa käsitellä henkilötietoja ainoastaan tietosuoja-asetuksessa säädetyllä perusteella. Henkilötietoja saa asetuksen mukaan käsitellä jos:

- rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
- käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
- käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
- käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Tietosuoja-asetuksen henkilötietojen käsittelyn oikeusperusteet eroavat osittain henkilötietolain 8 §:ssä mainituista perusteista. Toiminallisesti asetuksen oikeusperusteet vastaavat kuitenkin pitkälti henkilötietolain käsittelyn oikeusperusteisiin.

Erityisiä henkilötietoryhmiä koskevia tietoja ei lähtökohtaisesti lainkaan saa käsitellä. Asetuksen erityisen henkilötiedon määritelmä vastaa eräin muutoksin henkilötietolain arkaluonteisia henkilötietoja ja pitää sisällään tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisiä tai biometrisiä tietoja, joista henkilö voidaan yksiselitteisesti tunnistaa, terveyttä koskevia tietoja taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevia tietoja.

Erityisiin henkilötietoryhmiin kuuluvia tietoja voidaan käsitellä, jos asetuksessa erikseen mainittu peruste täyttyy. Erityisiä tietoja saa käsitellä mm. nimenomaisen suostumuksen perusteella, henkilön elintärkeiden etujen suojaamiseksi tai jos käsittely on tarpeen tärkeää yleistä etua koskevasta syystä lainsäädännön nojalla.

Mikäli erityisiä tietoja käsitellään, rekisterinpitäjä on vastuussa siitä, että kyseisiä tietoja käsitellään asetuksen poikkeussäännöksen mukaisesti.

Tietosuojaperiaatteet (artikla 5)

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista. Periaatteiden tavoitteena on ohjata henkilötietojen käsittelyä niin, että asetuksen vaatimukset toteutuvat ja rekisteröidyn oikeuksia kunnioitetaan.

Tietosuoja-asetuksen mukaan henkilötietojen käsittelyssä on noudatettava seuraavia periaatteita:

1. Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti sekä rekisteröidyn kannalta läpinäkyvästi.

   Läpinäkyvällä käsittelyllä tarkoitetaan sitä, että rekisteröidylle tulisi olla läpinäkyvää miten heitä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään tai on aikeissa käsitellä. Läpinäkyvyyden periaatteen mukaisesti henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä.

2. Henkilötietojen kerääminen tulee olla sidonnainen käyttötarkoitukseen, ja tietojen kerääminen tuleekin tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin tarkoitukseen, jolla ei ole sidonnaisuutta kerättyyn käyttötarkoitukseen.

   On kuitenkin katsottu, että mikäli tietoja käytetään myöhemmin arkistointitarkoitusta varten taikka tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei käyttötarkoitussidonnaisuutta tarvitse olla.

3. Henkilötietojen kerääminen tulee rajata ja minimoida tarpeelliseen tietoon suhteessa keräämisen tarkoitukseen ja henkilötietojen on oltava asianmukaisia sekä olennaisia.

   Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

4. Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä sekä rekisterinpitäjän on kohtuullisin toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

   Rekisterinpitäjän on varmistettava, esimerkiksi asetettujen määräaikojen avulla, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

5. Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin se on tarpeen tietojen käsittelyä varten. Tietoja voi kuitenkin säilyttää kauemmin, mikäli tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

6. Henkilötietoja käsittelyssä on varmistettava tietojen asianmukainen turvallisuus ja siten tietojen eheys ja luottamuksellisuus. Tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta, jossa on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

Osoitusvelvollisuus

Tietosuoja-asetuksen mukaan rekisterinpitäjän vastaa siitä, että periaatteita ja vaatimuksia noudatetaan. Tämän lisäksi rekisterinpitäjän on pystyttävä osoittamaan, että kyseisiä periaatteita ja vaatimuksia on noudatettu.

Rekisterinpitäjän on huolehdittava siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjän on etukäteen arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa ja dokumentoida tämä arviointi.

**Rekisterinpitäjän velvollisuudet**

Rekisterinpitäjän vastuu (artikla 24), sisäänrakennettu ja oletusarvoinen tietosuoja (artikla 25) ja riskiperusteinen lähestymistapa

Rekisterinpitäjä on tietosuoja-asetuksen mukaan vastuussa siitä, että se toteuttaa **tarvittavat tekniset ja organisatoriset toimenpiteet**, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia.

Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tilivalvontaa ja käytönvalvontaa, tietojen salausta, tietojen anonymisointia tai pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, käyttövalvontaa, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöä.

Toimenpiteiden riittävyys mitoitetaan riskiarvioinnin perusteella, jossa otetaan huomioon mm. käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit. Toimenpiteitä on arvioitava ja tarkistettava säännöllisesti ja ne on päivitettävä tarvittaessa.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaate edellyttää, että tietosuojaan liittyvät tarpeet ja vaatimukset tunnistetaan ja huomioidaan jo ennen käsittelyn aloittamista. Käytännössä tietosuojan tarpeet tulisi selvittää ja määrittää jo henkilötietojen käsittelyn suunnitteluvaiheessa ja esim. hankintatilanteessa jo ennen tarjouspyynnön tekemistä, eli silloin, kun määritellään toimintoja, prosesseja ja järjestelmien ominaisuuksia. Tietojärjestelmät, joissa käsitellään henkilötietoja, rakennetaan niin, että ne oletusarvoisesti toteuttavat tietosuojan periaatteet ja asetuksen vaatimukset.

Tietosuoja-asetuksessa omaksutun riskiperusteisen lähestymistavan mukaan asetuksessa vaaditut konkreettiset toimenpiteet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Rekisterinpitäjän on tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä, jotta se tämän arvion perusteella voi määritellä tarvittavat suojatoimet ja riskiin vastaavat muut organisatoriset ja tekniset toimenpiteet. 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.

Seloste käsittelytoimista (artikla 30)

Rekisterinpitäjän, henkilötietojen käsittelijän ja näiden edustajan on ylläpidettävä kirjallista ja sähköisessä muodossa olevaa selostetta kaikista henkilötietojen käsittelytoimista. Velvollisuus ei koske yhteisöä, jossa on alle 250 työntekijää, paitsi jos sen suorittama käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittelyn kohteena on erityisen arkaluonteisia tietoja.

Selosteesta on käytävä ilmi mm. henkilötietojen käsittelyn kannalta keskeisten tahojen yhteystiedot, käsittelyn kohteena olevien tietoryhmät ja tiedot henkilötietojen siirroista kolmansiin maihin. Siinä missä rekisteröidyille toimitettavat tiedot (eli rekisteriselosteet, ks. alla) ovat ulkoista käyttöä varten, tässä tarkoitettu seloste toimii ensisijaisesti rekisterinpitäjän, käsittelijän ja niiden edustajan sisäisenä työkaluna.

Vaikutustenarviointi ja ennakkokuuleminen (artiklat 35 ja 36)

Jos henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarvioinnissa arvioidaan käsittelyyn liittyvää riskiä ja rekisterinpitäjän keinoja vastata tähän riskiin. Asetuksessa on tarkempia säännöksiä riskin määrittelystä ja vaikutustenarvioinnin sisällöstä.

Vaikutustenarviointi on tehtävä erityisesti, jos käsittelyssä käytetään uutta teknologiaa tai jos 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.

Jos vaikutustenarvioinnin perusteella henkilötietojen käsittelyyn liittyvä riskin taso on korkea, eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi, on rekisterinpitäjän kuultava valvontaviranomaista ennen käsittelyn aloittamista (ennakkokuuleminen). Ennakkokuulemismenettely korvaa henkilötietolain mukaisen ilmoitusvelvollisuuden.

Tietosuojavastaavan tehtävä (artiklat 37, 38 ja 39)

Jokaisen viranomaisen ja julkishallinnon elimen, joka ei ole tuomioistuin, on nimitettävä tietosuojavastaava. Suomessa on aiemmin nimitetty tietosuojavastaavia sosiaali- ja terveydenhuollossa. Julkissektorin toimijoiden lisäksi myös muut toimijat, joiden ydintehtävät muodostuvat henkilötietojen käsittelystä, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai joiden ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomiota tai rikkomuksia koskeviin tietoihin ovat velvollisia nimittämään tietosuojavastaavia.

Tietosuoja-asetus sisältää yksityiskohtaiset säännökset tietosuojavastaavan asemasta ja tehtävistä ja EU-tasolla toimiva EU:n asiantuntijaryhmä WP 29 (Article 29 Working Party) on myös antanut tarkempaa ohjeistusta tietosuojavastaavista (linkki yleiskirjeen lopussa).

Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi nimittää yhteisen tietosuojavastaavan. Tietosuojavastaava voi tietosuojavastaavan tehtävän ohella suorittaa muita tehtäviä, mutta nämä tehtävät eivät saa aiheuttaa intressiristiriitoja.

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. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle.

Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Hänelle on asetuksen mukaan annettava riittävät resurssit sekä pääsyn henkilötietoihin ja käsittelytoimiin. Tietosuojavastaavalla on myös oikeus asetuksen perusteella resursseihin asiantuntemuksen ylläpitämiseksi.

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana.

Tietosuojavastaava antaa tietosuojaan liittyen tietoja neuvoja sekä työnantajalleen että muille työntekijöille henkilötietojen käsittelyyn liittyen. Hän seuraa asetuksen noudattamista omassa organisaatiossaan ja hänen vastuulleen kuuluu myös tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle organisaatiossa. Tietosuojavastaava neuvoo vaikutustenarviointeihin liittyen ja toimii valvontaviranomaisen yhteistyöpisteenä.

Henkilötietojen siirrot kolmansiin maihin (luku V)

Henkilötietojen siirrot ETA-alueen ulkopuolelle voidaan toteuttaa ainoastaan, jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tietosuoja-asetuksessa vahvistettuja edellytyksiä. Siirrot kolmansiin maihin aktualisoituvat esim. pilvipalvelun käytön yhteydessä. Pilvipalvelut saattavat käyttää ETA:n ulkopuolella sijaitsevia palvelimia. Myös pilvipalvelun tietojenkäsittelylaitteisto voi olla EU:n ulkopuolisen palveluntarjoajan hallinnassa. Molemmissa näissä tapauksissa henkilötietojen siirtojen pilvipalveluun täytyy tapahtua asetuksen kolmansia maita koskevien sääntöjen mukaisesti.

Henkilötietoja voidaan siirtää kolmanteen maahan ilman erityistä lupaa, jos komissio on päättänyt, että kyseinen kolmas maa varmistaa riittävän tietosuojan tason (siirto tietosuojan riittävyyttä koskevan päätöksen perusteella). Komissio julkaisee Euroopan unionin virallisessa lehdessä ja verkkosivustollaan luettelon niistä kolmansista maista, joiden osalta se on päättänyt, että tietosuojan taso on tai ei enää ole riittävä. Luettelo löytyy osoitteesta: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Henkilötietoja voi myös siirtää kolmanteen maahan, jos vastuussa oleva rekisterinpitäjä tai käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Asetus antaa tarkemmat määräykset mahdollisista suojatoimista ja mainitsee mm. viranomaisten välinen sopimus, sitovat säännöt, komission antamat vakiolausekkeet, hyväksytyt sertifiointimekanismit ja hallinnolliset säännökset. Lisäksi asetuksessa on säännöksiä erityistilanteita varten.

Henkilötietojen siirrot Yhdysvaltoihin toteutetaan tällä hetkellä Komission hyväksymän erillisen tietosuojasopimuksen, ns. Privacy Shield -sopimuksen turvin. Sopimuksessa hyväksytään yksittäiset yritykset turvallisina yhdysvaltalaisina yrityksinä ja henkilötietojen luovutuksensaajina.

Rekisteröidyn oikeudet

Avoin informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten (artikla 12)

Rekisterinpitäjän on suunniteltava toimintansa siten, että se voi pyynnöstä toimittaa rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Tietosuoja-asetuksen mukaan tiedot on pystyttävä esittämään tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa.

Artiklassa tarkoitetut tiedot ovat ainakin rekisteriselosteet; tarkastusoikeuden kohteena olevat tiedot; tiedot henkilötietojen korjaamisesta, poistamisesta, rajoittamisesta, siirrosta; tiedot käsittelyn tai profiloinnin vastustamisesta ja ilmoitukset tietoturvaloukkauksista.

Tiedot on toimitettava pääsääntöisesti kirjallisesti. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on myös pääsääntöisesti toimitettava sähköisesti. Tiedot voidaan pyynnöstä antaa myös suullisesti, jos rekisteröidyn henkilöllisyydestä on voitu luotettavalla tavalla varmistua.

Rekisteröidyn informoinnille ja toteutettaville toimenpiteille on asetettu määräaikoja. Tiedot annettava ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa.

Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän toimet rekisteröidyn oikeuksien toteuttamiseksi ovat pääsääntöisesti maksuttomia. Rekisterinpitäjä voi kuitenkin periä kohtuullisen maksun toimenpiteistään tai kieltäytyä pyynnön toteuttamisesta, jos rekisteröidyn pyyntö voidaan osoittaa kohtuuttomaksi tai ilmeisen perusteettomaksi. Kohtuuttomaksi tietopyynnöksi voitaisiin asetuksen mukaan katsoa esimerkiksi tapaukset, joissa rekisteröity tekisi toistuvia tietopyyntöjä ilmeisen perusteettomasti.

Toimitettavat tiedot eli rekisteriselosteet (artiklat 13 ja 14)

Tietosuoja-asetuksessa on yksityiskohtaisesti kuvattu ne tiedot, jotka rekisterinpitäjän tulee toimittaa rekisteröidylle henkilötiedot saatuaan. Käytännössä kyse on rekisteriselosteesta tai vastaavanlaisesta dokumentaatiosta, jonka sisältö kuitenkin on laajempi kuin nykyisen henkilötietolain mukaisten rekisteriselosteiden tiedot.

Artikla 13 sisältää luettelon tiedoista, jotka pitää ilmoittaa rekisteröidylle, jos tiedot henkilörekisteriin on kerätty rekisteröidyltä itseltään. Artikla 14 määrittelee tiedot, jotka on toimitettava silloin, kun tietoja ei ole saatu rekisteröidyltä itseltään. Tiedot on ilmoitettava rekisteröidylle, ellei asetuksesta muuta johdu. Tietoja ei esimerkiksi tarvitse antaa, jos rekisteröity on jo saanut nämä tiedot tai jos tiedot ovat salassa pidettäviä. Tietoja ei myöskään tarvitse antaa, jos tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa.

Jos henkilötiedot saadaan rekisteröidyltä itseltään, rekisteröidylle ilmoitettavat tiedot toimitetaan, kun henkilötiedot kerätään. Jos henkilötiedot saadaan muulta lähteeltä, rekisterinpitäjän on toimitettava asetuksessa mainitut tiedot rekisteröidylle kohtuullisessa ajassa, mutta viimeistään kuukauden kuluessa.

Rekisteröidyn oikeus saada pääsy tietoihin (artikla 15)

Rekisteröidyllä on kohtuullisin väliajoin oikeus saada pääsy henkilötietoihin, joita hänestä on kerätty sekä tietoihin hänen henkilötietojen käsittelyyn liittyen. "Kohtuullista väliaikaa" ei ole asetuksessa tarkemmin määritelty. Kaikilla rekisteröidyillä olisi siten oltava oikeus tietää ja saada ilmoitus erityisesti henkilötietojen käsittelyn tarkoituksista, käsittelyajasta, henkilötietojen vastaanottajista, käsiteltävien henkilötietojen automaattisen käsittelyn logiikasta sekä kyseisen käsittelyn mahdollisista seurauksista. Lisäksi rekisteröidyillä on oikeus saada tietoa omista oikeuksistaan suhteessa rekisterinpitäjään.

Rekisterinpitäjän pitää pyynnöstä ilmoittaa, käsitteleekö se kysyjää koskevia henkilötietoja. Jos henkilötietoja käsitellään, rekisteröidylle on annettava jäljennös rekisterissä olevista tiedoista, ellei ole lakisääteisiä perusteita olla antamatta pyydettyä tietoa.

Rekisteröidyn tiedonsaantioikeus koskee myös hänen henkilötietoihinsa kohdistuneita käsittelytoimia (kuka käsitellyt, mitä tietoja, milloin).

Pyydetyt tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Asetuksen mukaan rekisterinpitäjän on käytettävä kaikkia kohtuullisia keinoja tarkistaakseen sellaisen rekisteröidyn henkilöllisyyden, joka haluaa saada pääsyn tietoihin erityisesti verkkopalvelujen ja verkkotunnistetietojen yhteydessä. Rekisterinpitäjän täytyy riskilähtöistä lähestymistapaa käyttäen arvioida millä tavalla kysyjän henkilöllisyyttä arvioidaan sekä miten tiedot toimitetaan sähköisesti.

Oikeus tietojen oikaisemiseen (artikla 16)

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, esimerkiksi toimittamalla rekisterinpitäjälle lisäselvitystä.

Henkilötietojen oikaisua, poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus (artikla 19)

Tietosuoja-asetuksen mukaan rekisterinpitäjä on velvollinen ilmoittamaan tehdyistä henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisterinpitäjän on myös pyynnöstä ilmoitettava rekisteröidylle, keille tietoja on luovutettu.

Oikeus siirtää tiedot järjestelmästä toiseen (artikla 20)

Jos henkilötietojen käsittelyn oikeusperusta on suostumus tai sopimuksen täytäntöönpano ja käsittely suoritetaan automaattisesti, rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle. Tiedot on toimitettava jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Rekisteröidyllä on myös oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu.

Kun rekisteröity käyttää tätä oikeuttaan, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.

Yleisesti koneluettava muoto tarkoittaa esimerkiksi, että rekisteröityi saa tietonsa linkkinä.

Vastustamisoikeus ja automatisoidut yksittäispäätökset, ml profilointi (artiklat 21 ja 22)

Rekisteröidyllä on oikeus vastustaa käsittelyä suoramarkkinointitarkoituksissa ja eräissä muissa tietosuoja-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa.

Asetus ei kokonaan kiellä profiloinnin käyttöä. Vahvana lähtökohtana on kuitenkin, että rekisteröidyillä on oikeus olla joutumatta profiloinnin kohteeksi.

Tietoturvaloukkauksesta ilmoittaminen (artikla 33)

Rekisterinpitäjällä on velvollisuus ilmoittaa 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, riippumatta siitä, onko loukkaus tapahtunut omassa vai käsittelijän toiminnassa. 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. Asetuksessa on säädetty tarkemmin mitä rekisteröidyille toimitettava ilmoitus tulisi sisältää.

**Sopimusvaatimukset**

Tietosuoja-asetuksen artikla 28:n mukaan henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella. Jos rekisterinpitäjä ja henkilötietojen käsittelijä ovat eri tahoja, niiden välinen suhde täytyy asetuksen mukaan henkilötietojen näkökulmasta määritellä kirjallisessa sopimuksessa. Sopimuksessa vahvistetaan mm. käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät ja rekisterinpitäjän velvollisuudet ja oikeudet.

Asetus myös selkeästi määrittelee henkilötietojen käsittelijän roolin ja henkilötietojen käsittelijän suoraan lainsäädännöstä johtuvia velvoitteita on täsmennetty suhteessa henkilötietolain sääntelyyn. Asetuksen mukaan henkilötietojen käsittelijä ei esimerkiksi saa käyttää omia alihankkijoita käsittelyssä ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa (artikla 28.2).

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset. Esimerkiksi tarjouskilpailussa on toimittajan valinnassa kiinnitettävä huomiota toimittajan mahdollisuuksiin toteuttaa asetuksen ja rekisterinpitäjän asettamia tietosuojavaatimuksia.

Myös oletusarvoisen ja sisäänrakennetun tietosuojan vaatimuksella on sopimusvaikutuksia. Rekisterinpitäjän vastuulla on määritellä oman henkilötietotoiminnan käytännön vaatimukset. Ehdot näiden toteuttamiseksi on otettava sopimuksiin.

Asetuksen sopimusvaikutuksista seuraa, että sopimukset, joiden kohteena joko välittömästi tai välillisesti on henkilötietojen käsittely, täytyy uudelleenarvioida asetuksen muutosten näkökulmasta. Tällaiset sopimukset voivat olla esim. henkilöihin liittyvien palvelujen ulkoistamissopimukset; henkilöihin liittyvien palvelujen ostosopimukset; tietojärjestelmiin liittyvät sopimukset, mikäli tietojärjestelmissä käsitellään henkilötietoja; tai suora sopimus henkilötietojen käsittelystä toisen tahon kanssa.

**Seuraamukset ja hallinnolliset sanktiot**

Vahingonkorvaus (artikla 82)

Tietosuoja-asetuksen mukaan henkilöllä, jolle on aiheutunut tietosuoja-asetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta joko rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjällä on lähtökohtaisesti ns. ankara vastuu ja henkilötietojen käsittelijän vastuu on toissijaista. Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos se ei ole noudattanut rekisterinpitäjän lainmukaista ohjeistusta.

Hallinnolliset sakot (artikla 83)

Rekisteröidylle suoritettavan vahingonkorvauksen lisäksi rekisterinpitäjä ja henkilötietojen käsittelijä voivat joutua maksamaan hallinnollisia sakkoja tietosuoja-asetuksen rikkomisen perusteella. Hallinnollisen sakon määrä voi olla korkeintaan 20 000 000 euroa tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Hallinnollisen sakon määräämisestä päättää tietosuoja-asetuksen nojalla perustettu valvontaviranomainen. Valvontaviranomaisen organisaatio täsmennetään tulevassa tietosuojalaissa. Tietosuojalaki ottaa myös kantaa hallinnollisten sakkojen soveltamiseen viranomaistoimintaan.

Hallinnollisten sakkojen ohella tai niiden sijasta valvontaviranomaisella on käytettävissään useita muita keinoja rekisterinpitäjien ohjaamiseen ja lainvastaisen käsittelyn lopettamiseen. Tällaisia keinoja ovat esimerkiksi huomautus tai varoitus rekisterinpitäjälle, määräys saattaa käsittely lain mukaiseksi annetussa määräajassa, määräys korjata lainvastainen tilanne tai oikaista virheelliset tiedot, käsittelyrajoitusten asettaminen sekä määräys tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle.

**Suosituksia toimenpiteistä - miten varautua**

Tietosuoja-asetuksen mukaan tietosuojan painoarvo organisaatiossa korostuu. Tietosuojaan liittyy uudentyyppisiä vaatimuksia, riskejä ja tarpeita. Asetuksen velvoitteet vaativat myös resursointia. Tietosuoja-asetuksen vaatimukset on huomioitava systemaattisesti liiketoiminnan, palveluiden sekä tietojärjestelmien kehittämisessä, ml. hankinnoissa ja sopimuksissa, toiminnan organisonnissa ja johtamisessa. Huomiota tulisi myös kiinnittää tietosuojan dokumentointiin ja raportointiin.

Asetusta sovelletaan kansallisesti 25.5.2018 alkaen. Siirtymäaikana organisaatiossa tulisi oman toiminnan näkökulmasta selvittää asetukset vaatimat muutokset ja henkilötietojen käsittelyyn liittyvien prosessien kehittämistarpeita sekä saattaa toiminnot, prosessit ja sopimukset sellaiseen tilaan, että ne vastaavat asetuksessa säädettyjä ehtoja.

Esiselvitysvaiheessa tulisi ainakin:

- määrätä tietosuojaan liittyvien muutosten ja selvitysten vastuutaho
- selvittää henkilötietovarannot ja henkilötietojen käsittelyyn liittyvät prosessit
- päättää, mihin muutostyössä ensisijaisesti panostetaan
- tehdä riskiarvio, johon kuuluu mm. tietojärjestelmien muutostarpeet, sopimusvastuut, sanktio- ja vahingonkorvauksiin liittyvät riskit
- huolehtia henkilöstön osaamisesta, esimerkiksi koulutusten tai sisäisten ohjeiden avulla

Tietosuojavastaava voidaan nimittää myös etukäteen ja myös niissä organisaatioissa, joissa tietosuojavastaavan nimittäminen asetuksen mukaan ei ole pakollista.

**Tietoa muualla**

Tietosuojavaltuutetun toimisto, Oikeusministeriö: Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön selvityksiä ja ohjeita 4/2017.
(http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf)

Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) työryhmän raportti: EU-tietosuojan kokonaisuudistus, Vahti raportti 1/2016.
(https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229)

JUHTA asiantuntijaryhmän koulutukset ja työpajat v. 2017-2018.
(https://www.kuntaliitto.fi/ajankohtaista/2017/tulossa-tietosuojakoulutusta-ja-tyopajoja-eu-tietosuoja-asetukseen)

Tietosuojavaltuutettu. (http://tietosuoja.fi/fi/index/euntietosuojauudistus.html)

Working Party 29 Guidelines. (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

SUOMEN KUNTALIITTO

Hanna Tainio
varatoimitusjohtaja

Ida Sulin
lakimies