

EU-tietosuoja-asetus



EU:n perusoikeuskirja

- EU:n perusoikeuskirjan 8 artikla:
 1. Jokaisella on oikeus henkilötietojen suojaan.
 2. Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.
 3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

Tietosuoja-asetuksen tavoitteet

- Teknologian nopea kehitys ja globalisaatio ovat tuoneet henkilötietojen suojeluun uusia haasteita. Tietoa on enemmän saatavilla ja sen hyödyntäminen on helpompaa.
- Jotta digitaalinen talous voi kehittyä, tarvitaan tehokas tietosuoja koskeva lainsäädäntö, joka rakentaa luottamusta ja oikeusvarmuutta.
- Digitaalisten palvelujen myyminen luonnollisille henkilöille edellyttää heidän henkilötietojensa keräämistä. Luonnolliset henkilöt ovat valmiimpia luovuttamaan henkilötietonsa, kun he voivat luottaa siihen, että niitä käsitellään asianmukaisesti.

Voimaantulo

- EU-tietosuoja-asetus on annettu 27.4.2016.
- EU-tietosuoja-asetuksen soveltaminen kahden vuoden siirtymäajan jälkeen alkaa **25.5.2018**.
- EU-tietosuoja-asetus on Suomessa suoraan lakina voimassa, ei edellytä erillistä implementointia. Mikäli tietosuoja-asetus ja Suomen laki ovat ristiriidassa, sovelletaan tietosuoja-asetusta.
- Suomessa on käynnistetty laaja kansallisen lainsäädännön uudistustyö. Vanhoista laeista on poistettava tietosuoja-asetuksen kanssa ristiriidassa olevat säännökset. Lisäksi tietosuoja-asetus antaa useissa kohdin mahdollisuuden säätää kansallisessa lainsäädännössä asiasta toisin tai tarkemmin.

Soveltamisala (2 ja 3 art.)

- Henkilötietojen käsittely, joka on osittain tai kokonaan automaattista, sekä muussa kuin automaattisessa muodossa, jos henkilötiedot muodostavat rekisterin osan.
- Alueellinen soveltamisala: Henkilötietojen käsittely tapahtuu unionin alueella; tai käsittely liittyy tavaroiden tai palvelujen tarjoamiseen unionin alueella; tai käsittely liittyy rekisteröidyn käyttäytymisen seurantaan silloin, kun käyttäytyminen tapahtuu unionissa.
- Soveltamisalassa poikkeuksia kansallisen turvallisuuden ja rikosten ennalta ehkäisemisen ja tutkimisen osalta.

Henkilötiedon määritelmä (4 art.)

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 tai yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötietojen käsittelyn periaatteet (5 art.)

- Pitkälti samat kuin nykyisessä henkilötietolaissa:
 - Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
 - Käyttötarkoitussidonnaisuus
 - Tietojen minimointi
 - Täsmällisyys
 - Säilytyksen rajoittaminen (poikkeuksena yleisen edun mukainen arkistointitarkoitus)
 - Eheys ja luottamuksellisuus
 - Rekisterinpitäjän osoitusvelvollisuus
- Osoitusvelvollisuus on uusi käsite. Rekisterinpitäjän on pystyttävä osoittamaan, että tietosuoja-asetusta on noudatettu. Tämä edellyttää nykyistä laajempaa tapahtumien dokumentointia.

Käsittelyn lainmukaisuus (6 art.)

Henkilötietojen käsittely on lainmukaista, jos

- Käsittelylle on rekisteröidyn suostumus
- Käsittely liittyy sellaisen sopimuksen täytäntöönpanoon, jossa rekisteröity on osapuolena tai tällaisen sopimuksen tekemisen valmisteluun
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvollisuuden noudattamiseksi
- Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi
- Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen **oikeutettujen etujen toteuttamiseksi**, tätä voi rajoittaa rekisteröidyn perusoikeuden ja –vapaudet, erityisesti jos kyseessä on lapsi.

Lapsia koskevien tietojen käsittely (8 art.)

- Jos kyse on tietoyhteiskunnan palvelujen tarjoamisesta lapselle, on lapsen tietojen käsittely lainmukaista, jos lapsi on vähintään 16-vuotias. Jos lapsi on alle 16 vuotta, käsittelyyn on saatava vanhemman/huoltajan (vanhempainvastuunkantajan) suostumus.
- Jäsenvaltiot voivat säätää alemmasta iästä, lapsen on kuitenkin oltava vähintään 13-vuotias.

Erityiset henkilötietoryhmät (9 art.)

- Vastaavat osittain henkilötietolain arkaluonteisia tietoja
- Rotu tai etninen alkuperä, poliittinen mielipide, uskonnollisen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, terveyttä koskevat tiedot, seksuaalista käyttäytymistä tai suuntautumista koskevat tiedot
- Näitä tietoja saadaan käsitellä tiettyjen erityisehtojen täytyessä mm. jos henkilö on itse saattanut tiedot julkisiksi.
- Myös rikostuomioihin ja rikkomiseen liittyvien henkilötietojen käsittely on hyvin rajoitettua (10 art.).

Rekisterinpitäjän tiedonantovelvollisuus (13 art.)

Kerätessä tietoja rekisteröidyltä itseltään on toimitettava mm. seuraavat tiedot:

- Rekisterinpitäjän ja tämän edustajan identiteetti
- Tietosuojavastaavan yhteystiedot
- Henkilötietojen käsittelyn tarkoitus ja oikeusperuste
- Henkilötietojen vastaanottajat ja vastaanottajaryhmät
- Tieto siitä, jos tietoja aiotaan siirtää kolmanteen maahan ja tieto tietosuojan riittävydestä ja asianmukaisista suojatoimista
- Tietojen säilytysaika tai ajan määrittämiskriteerit
- Oikeus pyytää itseään koskevia henkilötietoja sekä oikeus pyytää tietojen oikaisemista ja poistamista
- Oikeus tehdä valitus valvontaviranomaisille
- Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus, onko rekisteröidyn pakko toimittaa tiedot ja tietojen antamatta jättämisen mahdolliset seuraukset

- Jos tiedot saadaan muulta kuin rekisteröidyltä itseltään, on pääsääntöisesti toimitettava vastaavat tiedot rekisteröidylle. (14 art.)
- Tiedonantovelvollisuutta ei kuitenkaan ole, jos
 - tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa; tällaisissa tapauksissa rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien, vapauksien sekä oikeutettujen etujen suojaamiseksi
 - Tietojen hankinnasta tai luovuttamisesta säädetään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä.
 - Tiedot on pidettävä luottamuksellisina, koska niihin kohdistuu lainsäädäntöön perustuva vaitiolovelvollisuus.

Rekisteröidyn oikeudet (15 – 22 art.)

Tietyin edellytyksin rekisteröidyllä on

- Oikeus saada pääsy tietoihin
- Oikeus tietojen oikaisemiseen
- Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Oikeus vastustaa henkilötietojen käsittelyä ja automaattisesti tehtäviä yksittäispäätöksiä

Seloste käsittelytoimista (29 art.)

- Jokaisen rekisterinpitäjän ja henkilötietojen käsittelijän on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Selosteessa on todettava mm.
 - Rekisterinpitäjän, rekisterinpitäjän edustajan, käsittelijän ja käsittelijän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
 - Käsittely tarkoitukset
 - Kuvaus rekisteröityjen ryhmästä ja henkilötietoryhmistä
 - Henkilötietojen vastaanottajien ryhmät
 - Tiedot henkilötietojen siirtämisestä kolmansiin maihin
 - Eri tietoryhmien poistamisen suunnitellut määräajat
 - Kuvaus teknisistä ja organisatorisista turvatoimista

Tietoturvaloukkauksista ilmoittaminen (33 ja 34 art.)

- Jos tapahtuu tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta valvontaviranomaiselle paitsi, jos loukkauksesta ei todennäköisesti aiheudu henkilöiden oikeuksiin tai vapauksiin kohdistuvaa riskiä.
- Tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos aiheuttaa todennäköisesti korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Tietosuojaa koskeva vaikutusten arviointi (35 art.)

- Jos toiminta aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, on rekisterinpitäjän toteutettava vaikutusten arviointi.
- Erityisesti tehtävä, jos
 - Kyse on luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällisestä ja kattavasta arvioinnista, joka perustuu automaattiseen käsittelyyn kuten profilointiin.
 - Kyse on laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita koskeviin tietoihin.
 - Kyse on yleisölle avoimen alueen järjestelmällisestä valvonnasta.

Tietosuojavastaava (37 -39 art.)

- Tietosuojavastaava on nimitettävä aina kun tietojen käsittelyä suorittaa julkishallinnon elin (ei tuomioistuin).
- Tietosuojavastaavaa nimitettäessä on otettava huomioon henkilön ammattipätevyys ja asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä.
- Tietosuojavastaava voi toimia työ- tai virkasuhteessa tai palvelusopimuksen perusteella.
- Tietosuojavastaavaa on tuettava antamalla tälle riittävät resurssit.
- Tietosuojavastaavalla on itsenäinen asema ja hän raportoi suoraan rekisterinpitäjän ylimmälle johdolle.

Riippumaton valvontaelin (51 – 59 art.)

- Kussakin jäsenvaltiossa yksi tai useampi riippumaton viranomaisen on vastuussa asetuksen soveltamisen valvonnasta
- Valvontaelin mm. neuvoo rekisterinpitäjiä ja käsittelijöitä, käsittelee rekisteröityjen valituksia, hyväksyy vakiosopimuslausekkeitä, hyväksyy käytännesääntöjä, osallistuu tietosuojaneuvoston toimintaa.
- Valvontaelimellä on laajat tutkintavaltuudet.
- Eri maiden valvontaelimet tekevät yhteistyötä.

Euroopan tietosuoja-neuvosto (68 – 76 art.)

- Muodostuu kunkin jäsenvaltion valvontaviranomaisen edustajasta ja Euroopan tietosuojavaaltuutetusta tai näiden edustajista.
- Riippumaton elin
- Neuvoa komissiota tietosuoja-asioissa, antaa suuntaviivoja, suosituksia ja parhaita käytänteitä, antaa lausuntoja kolmannen maan tietosuojan tason riittävydestä
- Neuvostolla on sihteeristö, jonka henkilöstöstä vastaa Euroopan tietosuojavaaltuutettu.

Vahingonkorvausvastuu (82 art.)

- Jos henkilölle aiheutuu asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta.
- Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut nimenomaisesti käsittelijälle osoitettuja asetuksen velvollisuuksia tai jos se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti.
- Käsitellään jäsenvaltion toimivaltaisissa tuomioistuimissa.

Hallinnollinen sakko (83 art.)

- Tämän asetuksen rikkomisesta voidaan määrätä hallinnollinen sakko yksittäisen tapauksen olosuhteiden mukaisesti ottaen huomioon mm rikkomisen luonne, vakavuus ja kesto sekä käsiteltyjen tietojen luonne.

- Sakon maksimimäärä on

enintään 10 000 000 euroa tai, jos kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta liikevaihdosta tiettyjen rikkomusten osalta

tai

enintään 20 000 000 euroa tai neljä prosenttia em. liikevaihdosta tiettyjen rikkomusten osalta.

- Jäsenvaltio voi asettaa sääntöjä siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä hallinnollisia sakkoja.

Virallisten asiakirjojen julkisuus (86 art.)

Viranomaiset yleisen edun vuoksi toteutetun tehtävän suorittamiseksi voivat luovuttaa viranomaisten hallussa olevien virallisten asiakirjojen sisältämiä henkilötietoja viranomaiseen sovellettavan unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti, jotta voidaan sovittaa yhteen virallisten asiakirjojen julkisuus ja tämän asetuksen mukainen oikeus henkilötietojen suojaan.

Sari-Anna Pennanen
Johtava kaupunginasiamies

040 3347257
sari-anna.pennanen@hel.fi

Oikeuspalvelut