

EU:n yleinen tietosuoja-asetus

Tietosuoja tarkoittaa ihmisten oikeutta omiin henkilötietoihinsa. Uusi EU:n laajuinen yleinen tietosuoja-asetus on nyt hyväksytty 14.4.2016 Euroopan parlamentin ja neuvoston päätöksillä.

Muutoksen tausta

Asetus tulee korvaamaan vuonna 1995 annetun henkilötietodirektiivin. Asetus sisältää säännökset mm. henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta, rekisteröiden suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä. Asetusta ryhdytään täysimääräisesti soveltamaan kahden vuoden siirtymäajan jälkeen, eli vuonna 2018.

Uuden tietosuoja-asetuksen tavoitteina ovat yksilön oikeuksien vahvistaminen, sisämarkkinaulottuvuuden lujittaminen, tietosuojan globaalin ulottuvuuden huomioiminen sekä tietosuoja sääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on luoda Euroopan unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Lisäksi pyritään parantamaan luottamusta online-palveluihin ja näin edistää EU:n digitaalista sisämarkkinoiden kehittämistä.

EU:n tietosuoja-asetus koskee lähtökohtaisesti kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa. Kyseessä on kaikissa jäsenvaltioissa suoraan sovellettava asetusta, joten eurooppalainen tietosuoja sääntely yhdenmukaistuu. EU:n tietosuoja-asetus tulee olemaan näin olleen olemaan suoraan sovellettavaa lainsäädäntöä Suomessa. Oikeusministeriö vastaa Suomessa asetuksen täytäntöönpanon edellyttämistä lainsäädäntötoimista. Joiltakin osin on mahdollisuus tarkentaa säännök-

siä kansallisessa lainsäädännössä. Suomen säännökset henkilötietojen käsittelystä voivat siksi olla myös jatkossa voimassa joillakin aloilla. Tämä koskee esimerkiksi henkilötietojen käsittelyä viranomaisissa.

Miten henkilötietojen käsittely muuttuu asetuksen myötä?

Lähtökohtana uudessa sääntelyssä on ollut ns. riskipohjainen lähestymistapa. Tarkoituksena on ottaa huomioon henkilötietojen käsittelyyn kulloinkin liittyvät riskit. Halutaan varmistaa rekisteröidyn suoja korkean riskin toiminnassa (huomioiden mm. tietojen laatu/luonne, käsittelytarkoitus ja laajuus), mutta toisaalta pyritään välttämään vähäriskisten toimien ylisääntelyä.

Uudella sääntelyllä halutaan ohjata yhteisöt ja yritykset ottamaan tietosuoja-asiat kokonaisvaltaisesti huomioon toimintansa suunnittelussa. Asetus patistaa rekisterinpitäjiä ja yrityksiä tarkistamaan tietosuojakäytäntöjensä lainmukaisuuden. Yritysten tulee myös varmistaa tietoturvasa riittävyys ja varautua ongelmatilanteisiin. Tietosuojavelvoitteensa laiminlyöville rekisterinpitäjille voidaan langettaa merkittäviä seuraamusmaksuja (10 000 000 – 20 000 000 euroa tai 2–4 % liikevaihdosta).

Rekisterinpitäjän on jatkossa noudatettava niin sanottua accountability-periaatetta (tilintekokykyisyys). Ei siis enää riitä, että rekisterinpitäjä passiivisesti noudattaa lakia (compliance), vaan rekisterinpitäjän on pystyttävä myös osoittamaan (tilintekovelvollisuus), että tietosuoja säännökset huomioidaan yhteisön tai yrityksen toiminnan suunnittelussa ja toteutuksessa. Tämä tarkoittaa mm. proses-

sien ja toimintatapojen entistä tarkempaa dokumentointia ja tietoturva- ja tietosuoja-asioiden hallinnollisen työn lisääntymistä jatkossa.

Erityisesti verkkoympäristössä henkilötietojen käsittelyyn liittyvät puutteet koetaan ongelmana asiain luotettavuuden ja käytettävyyden kannalta. Asiakkaiden ja sidosryhmien luottamus organisaation menettelytapoihin henkilötietojen käsittelyssä on toimintaa vahvasti tukeva tekijä. Riskien minimointi, hyvän maineen rakentaminen, kansalaisten ja kuluttajien luottamuksen säilyttäminen ovat asioita, joista on tulossa ratkaisevan tärkeitä kaikkien sektoreiden toiminnan menestymiselle.

Asetuksessa luetellaan rekisteröidyn eli henkilötietojen käsittelyn kohteena olevan henkilön oikeudet. Tällaisia oikeuksia ovat omia henkilötietoja koskeva tiedonsaantioikeus, oikeus saada tiedot oikaistua, oikeus tulla unohdetuksi sekä oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen. Lisäksi asetuksessa säädetään rekisterinpitäjien (eli tietojenkäsittelystä vastaavien) velvollisuudesta antaa rekisteröidyille avoimia ja helposti saatavia tietoja heidän tietojensa käsittelystä.

Asetus sisältää täsmennyksiä voimassa olevaan sääntelyyn sekä merkittäviä uusia veloituksia ja sanktioita. Eräitä asetukseen sisältyviä muutoksia:

- Entistä tarkempia määritelmiä erilaisista käsitteistä kuten suostumus, geneettiset tiedot, biometriset tiedot jne.

- Selkeämpiä sääntöjä henkilötietojen käsittelijöiden vastuusta, erityisesti rekisterinpitäjien, mutta myös rekisterinpidossa avustavien osalta.

- Asetuksen tullessa voimaan organisaatiolle ei riitä, että se noudattaa asetusta, vaan organisaation on pystyttävä osoittamaan, että tietosuojasäännökset huomioidaan rekisterinpitäjän toiminnassa.

- Ilmoitusvelvollisuus tietoturvaloukkausten tapautuessa.

- Tietosuojavastaavien asettaminen.

- Oikeus saada itseään koskevat tiedot koneluettavassa muodossa. Asetuksen mukaan rekisteröidyllä olisi oikeus siirtää henkilötietonsa ja kaikki muut

rekisteröidyn antamat tiedot toiseen järjestelmään silloin, kun rekisteröity itse on antanut henkilötiedot ja kun niiden käsittely perustuu suostumukseen tai sopimukseen.

- Asetuksella säädetään myös tietosuojaviranomaisen toimivallasta, tehtävistä ja valtuuksista. Ehdotuksen mukaan jokainen tietosuojaviranomainen on toimivaltainen oman jäsenvaltionsa alueella. Kun kyse on jäsenvaltioiden rajat ylittävistä henkilötietojen käsittelystä, on rekisterinpitäjän päätoimipaikan tietosuojaviranomainen yleensä toimivaltainen käsittelemään asiaa.

- Jäsenvaltioiden tietosuojaviranomaisten yhteistyötä varten asetuksella luodaan uusi ns. yhdenmukaisuusmekanismi ja yhden luukun mekanismi. Näin halutaan varmistaa se, että unionin uutta tietosuojasääntelyä sovelletaan yhdenmukaisesti kaikissa jäsenvaltioissa ja että ratkaisukäytäntö olisi mahdollisimman yhdenmukaista. Yhdenmukaisuusmekanismin keskeinen toimija on asetuksella perustettava Euroopan tietosuojaneuvosto (EDPB), jolla on mahdollisuus antaa sitovia päätöksiä tietosuoja-asetuksen soveltamisesta.

- Valvontaviranomaisella on valtuudet langettaa hallinnollisia seuraamuksia asetuksessa luetelluista teoista määräämällä sakkoja tiettyyn enimmäismäärään asti kuhunkin tapaukseen liittyvät olosuhteet asianmukaisesti huomioon ottaen.

Lisätietoa:

Tietosuojavaltuutettu: www.tietosuoja.fi

[EU:n tietosuoja-asetuksen suomennos \(huhtikuu 2016\)](#)