Uusi tietosuoja-asetus 2016 – vaatimukset yhteisöille ja henkilökunnalle?

Teppo Laine

Asianajaja, osakas

Legistum

Tietosuojan kolme ulottuvuutta

Juridisesti voidaan katsoa, että uusi tietosuoja-asetus sisältää kolme ulottuvuutta:

1. Käsittelyn tietoturva
    1. Tiedon tekninen suojaaminen
    2. Tiedon säilytyksen valvonta
2. Inhimillinen tietosuoja
    1. Mikään järjestelmä ei auta, jos ihminen vuotaa
    2. Osaamisen lisääminen, huolimattomuusvirheiden tekninen estäminen ja tahallisten tietovuotojen havaitseminen ja torjunta
    3. Ihminen on riski!
3. Hallinnollismenettelylliset vaatimukset
    1. Juridinen osaaminen
    2. Prosessit ja organisatoriset resurssit

Legistum

Tietosuojan riskit

Riskit voi karkeasti jakaa kolmeen ryhmään:

1. Tekniset riskit, suojausten puutteellisuus, laite- ja salasanaturvallisuus, käytettävät järjestelmät

2. Inhimilliset riskit, osaamispuutteet, ”oikominen”, salasanojen ja laitteiden käyttö ja säilytys

3. Fyysiset riskit, murtoriskit, arkistojen / asiakirjojen säilytys ja tuhoaminen, erityistilanteet, kuten muutot, asiakastilat, sisäinen tietosuoja asiakirjahallinnassa

Legistum

Käsittelyn lainmukaisuusvaatimus tarkentuu

Käsittelyn lainmukaisuus

1. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

a)rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;

b)käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;

c)käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;

Legistum

Käsittelyn lainmukaisuusvaatimus tarkentuu

Käsittelyn lainmukaisuus (jatkuu)

d)käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;

e)käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;

f)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.

Ensimmäisen alakohdan f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.

Legistum

Rekisterit

- Ensin selvitetään, mitä henkilöstörekistereitä meillä on
  - Henkilörekisteri on rekisteri, josta yksilö on tunnistettavissa
  - Tarkoittaa luonnollisia henkilöitä eli ihmisiä
  - Käsite on siten laaja
- Tarkistetaan, mitä tietoa on kerätty
- Tarkistetaan tiedon keräämisen perusteen olemassaolo
- Tarkistetaan tietojen oikeellisuus ja ajantasaisuus
- Poistetaan perusteettomat, tarpeettomat, virheelliset ja vanhentuneet tiedot
- Tarkistetaan tietojen suojauksen taso
- Selvitetään henkilöstön pääsy tietoon, rajoitetaan vain niille, joilla tarve päästä tietoon

Legistum

Arkaluontoiset tiedot

- Erityinen huomio tulee kiinnittää arkaluontoisten tietojen käsittelyyn:

- Yksilön henkilöön liittyvät tiedot (uskonto, etninen tausta, sukupuolinen suuntautuminen, poliittinen näkemys ym.)
- Terveystiedot
- Taloustiedot (ulosoton asiakkuus)
- Viranomaistiedot (rikosrekisteri tms.)
- Henkilökohtaiset tiedot (harrastukset tms.)

Legistum

Tyypillisiä rekistereitä

- Sähköiset rekisterit:
  - Toiminnanohjausjärjestelmä
  - Jäsen-, asiakas-, markkinointi-, asiakaspalvelu- ja sopimusrekisterit
  - Kirjanpito- ja laskutusohjelma
  - Henkilöstö- ja palkkakirjanpitorekisteri
  - Opinto- tms. rekisteri
  - Valokuva-arkistot, valvontakameratallenteet jne.
- Manuaaliset rekisterit
  - Paperiarkistot, sairaslomatodistuskansiot, arviointi- ja kehityskeskustelukansiot, viranomaisilmoitukset
- ”Piilorekisterit
  - Sähköpostit, puhelimen yhteystiedot, tekstiviestit, whats upit, opintojen seurantaohjelmat jne.
  - ”Omat rekisteröidyt muistiinpanot

Legistum

EU:n yleinen tietosuoja-asetus pakottaa yhteisöt muuttamaan toimintamallejaan – uusia oikeuksia yksityisille

- ✓ EU:n tietosuoja-asetus merkitsee radikaaleja tiukennuksia yksityisyyden suojaan sekä yhteisöjen ja yritysten tietosuojavelvoitteisiin

- **pääsy omiin tietoihin helpottuu**: ihmiset saavat enemmän tietoa siitä, miten heidän tietojaan käsitellään, ja tämä tieto on annettava heille selkeällä ja ymmärrettävällä tavalla;

- **oikeus siirtää tiedot järjestelmästä toiseen** henkilötiedot on entistä helpompi siirtää palveluntarjoajalta toiselle;

Legistum

EU:n yleinen tietosuoja-asetus pakottaa yritykset muuttamaan toimintamallejaan – uusia oikeuksia yksityisille

- entistä selkeämpi ”**oikeus tulla unohdetuksi”**: kun käyttäjä ei enää halua, että hänen tietojaan käsitellään, tiedot poistetaan, paitsi jos on olemassa jokin laillinen peruste säilyttää ne;

- **oikeus saada tieto siitä, että omiin tietoihin on murtauduttu**: esimerkiksi yritysten ja organisaatioiden on ilmoitettava kansalliselle tietosuojaviranomaiselle vakavista tietosuojaloukkauksista mahdollisimman pian, jotta käyttäjät voivat toteuttaa tarvittavat toimenpiteet.

Legistum

EU:n yleinen tietosuoja-asetus pakottaa yhteisöt muuttamaan toimintamallejaan

Jatkossa ei riitä, että noudatetaan lakia, vaan on pystyttävä osoittamaan, että tietosuojasäännökset huomioidaan yhteisön tai yrityksen toiminnan suunnittelussa → todistustaakka kasvaa

- Todistustaakka tietosuojakysymysten lainmukaisesta hoidosta tulee lankeamaan yrityksille, **joista pyritään tekemään huomattavien sakkojen uhalla tilintekovelvollisia**

- Asetuksen mukaan valvontaviranomaisella olisi siis valtuudet langettaa hallinnollisia seuraamuksia asetuksessa luetelluista teoista määräämällä sakkoja tiettyyn enimmäismäärään asti kuhunkin tapaukseen liittyvät olosuhteet asianmukaisesti huomioon ottaen

Legistum

Uusia velvollisuuksia

1.Jokaisen tiedon kohdalta on pystyttävä näyttämään, että sen keräämiseen on saatu rekisteröidyn **henkilön suostumus tai jokin muu edellytyksistä on täyttynyt.**

2.Tietosuojavelvoitteensa laiminlyöville yrityksille voidaan langettaa merkittäviä seuraamusmaksuja.

➢ Sanktioitavat teot on jaettu kolmeen luokkaan, joissa sakon määrä voi olla enintään ***10 miljoonaa tai 20 miljoonaa euroa.*** Tämän lisäksi sakko voidaan määrätä kokonaisliikevaihdon perusteella → sakon määrä 2 / 4 % liikevaihdosta

➢Sakkojen ohella on käytettävissä myös lievempiä keinoja, kuten kirjallinen huomautus

Legistum

Uusia velvollisuuksia

4. Tietyistä tietoturvaloukkauksista **on ilmoitettava → ilmoitusvelvollisuus**

5. **Tietosuojavastaavan nimeämisen** vaatimus tulee laajentumaan tämän hetkisestä

6.Tietojen käsittelystä tulee informoida käyttäjää entistä selkeämmin ja ymmärrettävällä tavalla.

- Informaation on oltava helposti saatavilla ja se tulee tehdä ennen tiedon keräämistä ja/tai palvelun käyttöönottoa

Legistum

Valmistautuminen asetuksen voimaantuloon

Toimenpiteet:

1.Omien rekisterien selvitys, mitä, missä ja millaisia?

- Selvitetään missä rekistereitä ja millaisia on
- Kerätään ne kootusti yhteisön ”haltuun”
- Puhdistetaan tarpeeton pois

2.Riskiarvio, millaista tietoa, mitä riskejä

3.Suunnitelma tietosuojan ja tietoturvan tason varmistamiseksi

4.Tietosuojaohjeet

5.Henkilöstön koulutus

6.Toimenpiteiden vaikutusten arviointi

7.Tietosuojan valvonta

8.Puuttuminen väärinkäytöksiin, sanktiot, rajoitukset

Legistum

KIITOS TARKKAAVAISUUDESTANNE!

Teppo Laine

Asianajotoimisto Legistum Oy
Vilhonkatu 9 C.
FI-00100 Helsinki

Puh. 040 047 4074
teppo.laine@legistum.fi

Legistum