TIETOSUOJA-ASETUS GDPR 25.5.2018

- Jokaisella yrityksellä on ainakin vähintään yksi asiakas ja siellä yhteyshenkilö, joten tämä koskee kaikkia yrityksiä niiden koosta riippumatta. Lisäksi jos yrityksellä on vähintään yksikin työntekijä, asetus tulee sovellettavaksi.

- Jokaisen yrityksen olisi tarkasteltava nykyhetken asiakasrekisteriänsä ja miettiä, että mistä tietoja hankitaan, miten niitä käsitellään ja mihin niitä luovutetaan.

- Rekisterissä oleviin tietoihin on aina oltava laillinen peruste ja ne on oltava tarpeellisia eli ei ns. ”kiva tietää” – tietoja.

- Yrityksiä koskevat tiedot eivät ole henkilötietoja eikä tietosuoja-asetus sovellu niihin lainkaan. Sen sijaan yrityksen yhteyshenkilön nimi- ja muut henkilötiedot ovat asetuksen tarkoittamia henkilötietoja.

- Esimerkiksi asiakasyrityksen puolesta toimivat yhteys- tai muut henkilöt ovat rekisteröityjä ja heidän nimi, osoite ja puhelinnumero ovat asetuksen tarkoittamaa henkilötietojen käsittelyä.

- Suurin osa tietosuoja-asetuksen velvoitteista koskee rekisterinpitäjää eli yritystä, joka päättää mitä henkilötietoja kerätään sekä miten ja mihin käyttötarkoituksiin niitä käytetään.

- Henkilötietojen käsittelijä on esimerkiksi alihankkija tai yhteistyökumppani, joka käsittelee henkilötietoja nimenomaan päämiehensä puolesta tai lukuun. Käsittelijä ei päätä tietojen keräämisestä vaan sen tekee rekisterinpitäjä. Henkilötietojen käsittelijä voi käsitellä henkilötietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti.

- Sekä rekisterinpitäjän että henkilötietojen käsittelijän on kartoitettava tietoturvaan liittyvät riskit ja pyrittävä ne ehkäisemään.

- Jos yrityksen käsittelemiin henkilötietoihin kuuluu arkaluonteisia henkilötietoja tai jos yritys käsittelee esimerkiksi lasten henkilötietoja, täytyy tietojen käsittelyyn kiinnittää erityistä huomiota.

Erityisiä henkilötietoja eli arkaluonteisia tietoja ovat:

- rotu tai etninen alkuperä
- poliittiset mielipiteet
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettiset ja biometriset tiedot, joita käsitellään henkilön tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalinen käyttäytyminen ja suuntautuminen.

- Arkaluonteiselle henkilötietojen käsittelylle on aina oltava erityinen peruste: rekisteröidyn suostumus, arkaluonteisten tietojen käsittely sallitaan työlainsäädännössä tai tietojen käsittely on tarpeen oikeusvaateen takia.

- Asetuksessa on määritelty, että rekisteröidyllä on mm. oikeus saada pääsy omiin tietoihin, oikeus pyytää oikaisua virheellisiin tietoihin ja oikeus pyytää, että omat tiedot poistetaan kokonaan.

- Tietosuoja-asetuksen mukaan henkilötietojen käsittelyn tulisi olla läpinäkyvää ja rekisteröityjen tulisi saada tieto siitä, miten heitä koskevia henkilötietoja kerätään ja käytetään sekä siitä, missä määrin henkilötietoja käsitellään tai tullaan käsittelemään. Tietojen on oltava helposti saatavilla ja tiedot on annettava yksinkertaisella ja selkeällä kielellä.

- Käytännössä yritys voi laatia tietosuojaselosteen, jossa on helpointa kuvata henkilötietojen käsittelyyn liittyvät asiat.

- Henkilötietojen käsittely tapahtuu usein monen eri toimijan yhteistyönä. Tällöin on hyvä laatia tietojenkäsittelysopimus, jossa huomioidaan molempien osapuolten tosiasialliset tarpeet ja vastuut. Selkeästä sopimuksesta on hyvä löytyä ainakin

    - henkilötietojen käsittelyn kohde ja kesto
    - käsittelyn luonne ja tarkoitus
    - mitä henkilötietoja käsitellään (esim. nimet ja palkkatiedot)
    - rekisteröityjen ryhmät (esim. rekisterinpitäjän asiakkaat/työntekijät)
    - rekisterinpitäjän velvollisuudet

- Henkilötietojen käsittelijän tulee varmistaa, että ne henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee lakisääteinen salassapitovelvollisuus.

- Tietosuoja-asetus tuo valvontaviranomaiselle uuden valtuuden määrätä hallinnollisia sakkoja. Jos velvoitteita rikkoo perustavanlaatuisesti, sakkojen enimmäismäärä on 20 miljoonaa euroa tai 4 % yrityksen liikevaihdosta (kumpi näistä määristä on suurempi). Lievemmistä rikkomuksista määrättävät hallinnollisten sakkojen enimmäismäärä on 10 miljoonaa euroa tai 2 % liikevaihdosta.