

Liite 2. Tuusulan tietoturva- ja tietosuojapolitiikka

Rekisterinpitäjän velvollisuudet

EU:n yleinen tietosuoja-asetus (679/2016) edellyttää rekisterinpitäjältä seuraavien velvoitteiden huomioimista henkilötietojen käsittelyssä:

1) Tietosuojaperiaatteiden noudattaminen

Henkilötietoja on tietosuoja-asetuksen mukaan käsiteltävä siten, että kaikissa tiedon käsittelyvaiheissa varmistetaan

- ✓ käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- ✓ käyttötarkoitussidonnaisuus
- ✓ tietojen minimointi
- ✓ tietojen täsmällisyys
- ✓ tietojen säilytyksen rajoittaminen
- ✓ tietojen eheys ja luottamuksellisuus

2) Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet edellyttävät, että tietosuoja koskevat kysymykset tunnistetaan ja otetaan huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja tai kehitetään tietojärjestelmiä.

3) Osoitusvelvollisuus

Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia. Kuten sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden, myös osoitusvelvollisuuden ja rekisterinpitäjän vastuun toteuttamiseksi rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että asetusta noudatetaan.

4) Ilmoitusvelvollisuus

Rekisterinpitäjän tulee ilmoittaa henkilötietojen tietoturvaloukkauksesta 72h kuluessa valvontaviranomaiselle, mikäli loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Myös rekisteröidylle on ilmoitettava tietoturvaloukkauksesta viipymättä, mikäli tapahtunut voi aiheuttaa uhkaa rekisteröidyn yksityisyyden suojalle. Kaikista (myös matalan riskin) tietoturvaloukkauksista on laadittava organisaation sisäinen dokumentaatio.

5) Tietosuojan vaikutustenarviointi

Kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on tietosuoja-asetuksen mukaan rekisterinpitäjän tehtävä tietosuoja koskeva vaikutustenarviointi. Riskin tasoa arvioitaessa on otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitus.

6) Rekisteröidyn informoiminen ja henkilötietojen käsittelyperusteen määrittäminen

Rekisterinpitäjän tulee informoida rekisteröityä henkilötietojen käsittelystä, sekä määrittää henkilötietojen käsittelyperuste. Ao. tiedot voidaan esittää esimerkiksi rekisterikohtaisesti laaditussa tietosuojaselosteessa.