

EU:n Tietosuoja-asetus ja siihen valmistautuminen

EU:n tietosuoja-asetus

- EU:n tietosuoja-asetus 2016/679
GDPR (General Data Protection Regulation)
korva Suomessa vuodesta 1999 voimassa olleen
henkilötietolain.
- Asetus on jo voimassa ja siirtymaika päättyy 25.05.2018
- Koskee yrityksiä joilla on näitä:
 - Työntekijöitä
 - Työnhakijoita
 - Asiakkaita
 - Toimittajia
 - Yhteistyökumppaneita



Uudistuksen tavoitteita

- Parantaa yksityishenkilöiden henkilökohtaisten tietojen suojaa.



Hakkerit varastivat 143 miljoonan ihmisen henkilötiedot Yhdysvalloissa – tietoja epäillään käytettävän identiteettivarkauksiin

Henkilötietovarkaus sai luopumaan tulosteista

- Luoda edellytyksiä EU:n sisäisille digitaalisille markkinoille.
- Yhtenäistää sääntelyä EU:ssa.

Rekisterinpitäjän huolehdittava

- Tietosuojaperiaatteita noudatetaan kaikissa käsittelyvaiheissa
 - Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
 - Käyttötarkoitussidonnaisuus
 - Tietojen minimointi
 - Tietojen täsmällisyys
 - Tietojen säilytyksen rajoittaminen
 - Tietojen eheys ja luottamuksellisuus
 - Rekisterinpitäjän osoitusvelvollisuus
- Pystyttävä osoittamaan periaatteiden noudattaminen
- Periaatteiden noudattamisen osoittaminen edellyttää tietojen käsittelyn tarkkaa suunnittelua ja dokumentointia

Uusia oikeuksia ja velvollisuuksia

- Rekisteröidylle oikeus saada pääsy omiin tietoihin
- Rekisteröidylle oikeus tulla unohdetuksi
- Rekisteröidylle oikeus siirtää tiedot toiseen järjestelmään
- Rekisterinpitäjälle tietomurtojen tiedottamisvelvollisuus
- Rekisterinpitäjälle osoitusvelvollisuus
- Rekisterinpitäjälle sakko jopa 4 % liikevaihdosta tai 20 M €

Henkilötietojen määritelmä

- Henkilötiedoilla 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, valokuvan, videotallenteen, sijaintitiedon, verkkotunnistetietojen/IP-osoitteen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Esimerkkejä tallennuspaikoista

- Mobiililaitteet, tabletit ja tietokoneet, palvelimet sekä pilvipalvelimet.
 - Sähköpostit
 - Excel- ja Word-tiedostot
- Taloushallintajärjestelmä
- Paperiarkistot
- Skannatut dokumentit
- Valokuvat
- Valvontakameradata



Dokumentoinnin kolme tasoa

1. Poliitiikka (Policy)

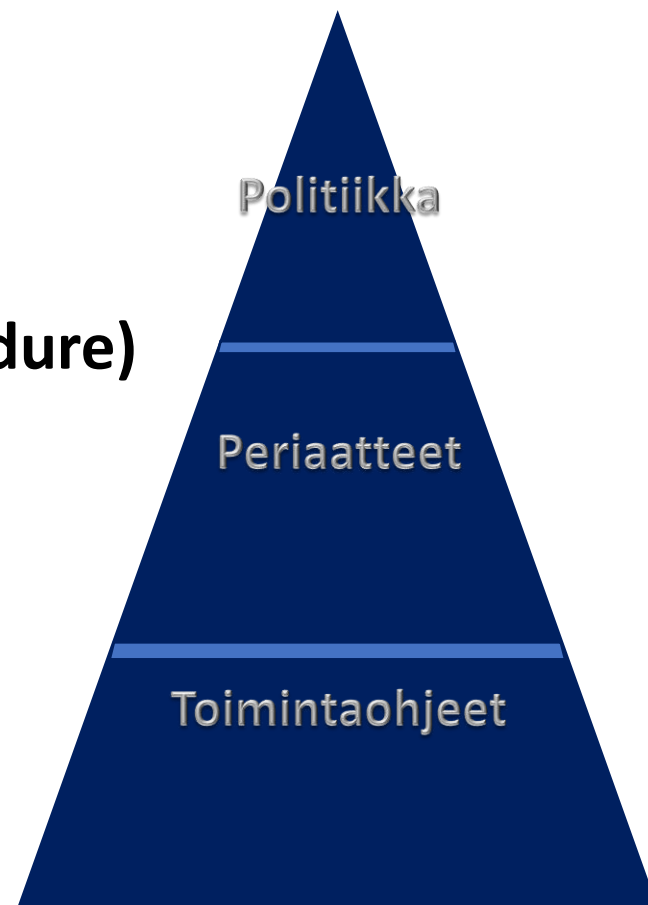
Johdon kannanotto tietoturvallisuuden ja tietosuojaan puitteille, linjauksille ja vastuille.

2. Periaatteet (Std Operating Procedure)

Kuvaa (politiikkaa tarkemmin) organisaation käytännön toteutusta ja määrämuotoisia toimintatapoja.

3. Toimintaohjeet (Guidelines)

Organisaation yksityiskohtainen ohjeistus tietoturva- ja tietosuoja-asioiden käsittelyyn ja käytännön toimintaan.



Dokumentoitava mm.

- Kuka käsittelee, kuinka käsittelee, miksi käsittelee
- Millaista henkilötietoa käsitellään, millä oikeutuksella
- Missä henkilötieto säilytetään
- Rekisteri-/tietosuojaselosteet
- Käyttövaltuusohjeet, lokiohjeet, varmistamispolitiikka
- Tietosuojapolitiikka, -periaatteet ja toimintaohjeet
- Tietoturvapoliittikka, -periaatteet ja toimintaohjeet
- Varautuminen odottamattomaan ja ylläpitosuunnitelma
- Ohjeet ulkoiseen tiedottamiseen

Määriteltävä ja toteutettava

- Henkilötietojen luokittelu
 - julkinen
 - sisäinen
 - luottamuksellinen
 - erittäin luottamuksellinen
- Tietoturva-profiili tietokoneisiin ja mobiililaitteisiin
- Tietojen ja liikenteen salaaminen
- Järjestelmien suojauksen varmistaminen
- Pääsyoikeuksien rajaaminen ja hallinta
- Fyysisestä turvallisuudesta huolehtiminen (tilat, laitteet)

Oman toiminnan kehittäminen

- Henkilötietoja käsitellään vähintäänkin luottamuksellisina
- Omilta koneilta henkilötieto-tiedostot yrityksen levyjaolle
- Tavallisella sähköpostilla ei lähetetä arkaluontoista tietoa
- Käytä kirjautumisessa riittävän haastavaa salasanaa
- Lukitse tietokone kun poistut sen ääreltä (Windows-painike + L)
- Ovet ja ikkunat pidetään lukittuina kun poistut tilasta
- Työlaite on vain henkilökohtaiseen käyttöön
- Huomioi tietokoneen ja puhelimen turvallinen säilyttäminen
- Puhelimessa oltava pin-koodi ja/tai sormenjälkilukija käytössä