

TIETOSUOJATYÖN ORGANISOINTI

2016



OpiTietosuoja.fi

Noviisista Mestariksi

Nosta
tietosuoja
koko johdon
agendalle!

Organisoi
tietosuojatyö
ja nimeä
tietosuoja-
vastaava

Systematsoi
henkilötietojen
käytönvalvonta

Varaudu
riskeihin
sopimuksilla
ja
vakuutuksilla

Tieto on
arvokasta –
MasterDatan
hallinta
tärkeää

Ota tietosuoja
mukaan
organisaation
kokonais-
arkkitehtuuriin

Panosta
henkilöstön
kouluttamiseen

Seuraa ja
kehitä –
Laadi
Tietotilin-
päättös

Lähtökohtia

- Nykytilan kartoitus
- Henkilörekisterihallinnon järjestäminen
- Kirjalliset politiikat, periaatteet ja ohjeet ("privacy by design"-periaatetta tukeva)
- Riittävät resurssit
 - Tietosuojapäällikön/tietoturvapäällikön/tietosuojavastaavien nimeäminen ja tehtävien/aseman määrittely
 - Tietosuojaryhmän perustaminen ja tehtävien määrittely
- Riskienhallinta
 - Riskien tunnistaminen ja luokittelu
 - Riskianalyysit
 - Toimintaohjeet riskien toteutuessa
 - Kirjalliset sopimukset palveluja ostettaessa (turvallisuusliitteet, raportointivelvoitteet, salassapitositoumus, rekisterinpito, asiakastietojen käsittely, alihankkijoiden alihankkijat jne.)
- Seuraamuskäytännöt tietoturva- ja tietosuojarikkomuksissa
- Tietosuojattavan jätteen hävitysprosessin järjestäminen
- Tietoturvan ja tietosuojan omavalvontasuunnitelma
- Tietotilinpäätös ("accountability"-periaatetta tukeva)



Johdon vastuu – Varmista perusedellytykset

- 1) Nosta tietoturva- ja tietosuoja johdon agendalle ja pidä se siellä
- 2) Nimeä avainhenkilöt ja varmista riittävä resursointi
- 3) Laadi pelisäännöt
- 4) Panosta henkilöstön kouluttamiseen
- 5) Seuraa ja kehitä, sekä puutu poikkeamiin



Rooleista -mitä ne voisivat pitää sisällään?

Tietosuojaryhmä

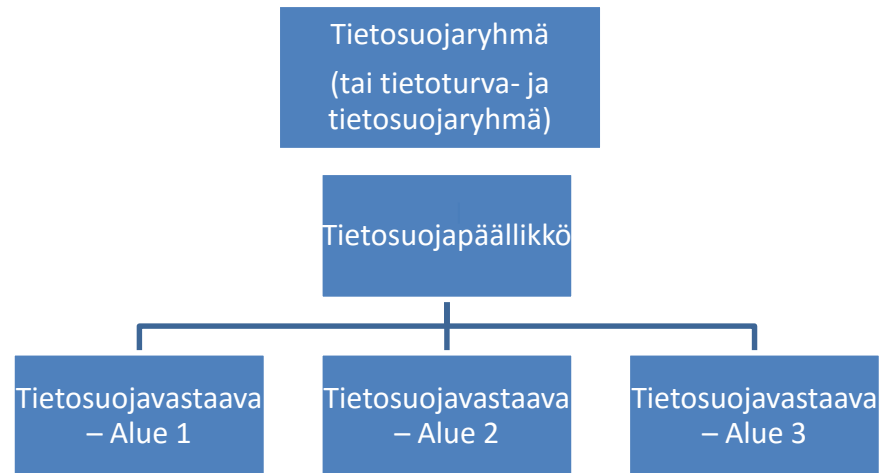
- Näkyvyys kokonaisuuteen
- Asioiden suunnittelu
- Raportointi

Tietosuojapäällikkö

- Kokonaisvastuu koordinoinnista
- Johdon erityisasiantuntija
- Yhteys valvontaviranomaisiin

Tietosuojavastaava(t)

- Vastuu sovitusta osa-alueesta
- Henkilöstön kouluttaminen
- Määrä organisaation koon mukaan



TIETOSUOJATYÖN TOTEUTTAMINEN

-vaatii yhteistyötä

- Johdon tukena toimiminen
- Henkilötietojen oikeaoppisen käsittelyn suunnitteluvuorokauden noudattaminen
- Lainsäädännön muutoksien seuraaminen ja tiedottaminen
- Ohjeiden laatiminen ja jalkauttaminen
- Henkilöstön perehdytysprosessin varmistaminen
- Henkilöstön kouluttaminen ja auttaminen
- Henkilöstön osaamisen mittaaminen
- Henkilötietojen käsittelyn valvonta
- Tietosuojajoihtimien raportointi johdolle
- Tietotilinpäätöksen määrämuotoinen kokoaminen
- Vaikuttavuusarvioiden laatiminen (eng. PIA)
- Yhteydenpito valvontaviranomaisiin



Tietotilinpäätös vs. tilintekokykkyisyys

Tietotilinpäätös on hyvä tapa systemaattisesti seurata ja kehittää organisaation tietopääoman käyttöä

- tietosuojaan näkökulmasta se tarjoaa hyvän rakenteen seuraamiseen
- Pystyt osoittamaan noudattavasi mm. EU:n tietosuoja-asetuksen mukana tuomia velvoitteita
- kansallisesti oli hyvä määritellä yhteinen mittaristo (vertailukelpoisuus)

Esimerkkejä mittareista

- tietoturva- ja tietosuojapojikkeamat
- tietojärjestelmien käyttökatkot
- käytönvalvontasuunnitelman toteutuminen
- tietoturvan ja tietosuojaan omaavaltontasuunnitelman toteutuminen
- tietosuoja- ja tietoturvarikkomukset
- mahdolliset viranomaisten selvityspyynnöt
- lakimuutokset
- tietosuoja- tietoturvakoulutukset
- ohjeistukset



Tietosuojaosaaminen on tuottavuuden menestystekijä

