TIETOSUOJATYÖN ORGANISOINTI

17.3.2018

OpiTietosuojaa.fi
Noviisista Mestariksi

OpiTietosuojaa.fi
Noviisista Mestariksi

Tietosuoja on mm.

- Henkilötietojen oikeaoppista käsittelyä
- Digitalisaation mahdollistaja
- Kaikkien osapuolten oikeusturvaa
- Riskienhallintaa
- Maineenhallintaa

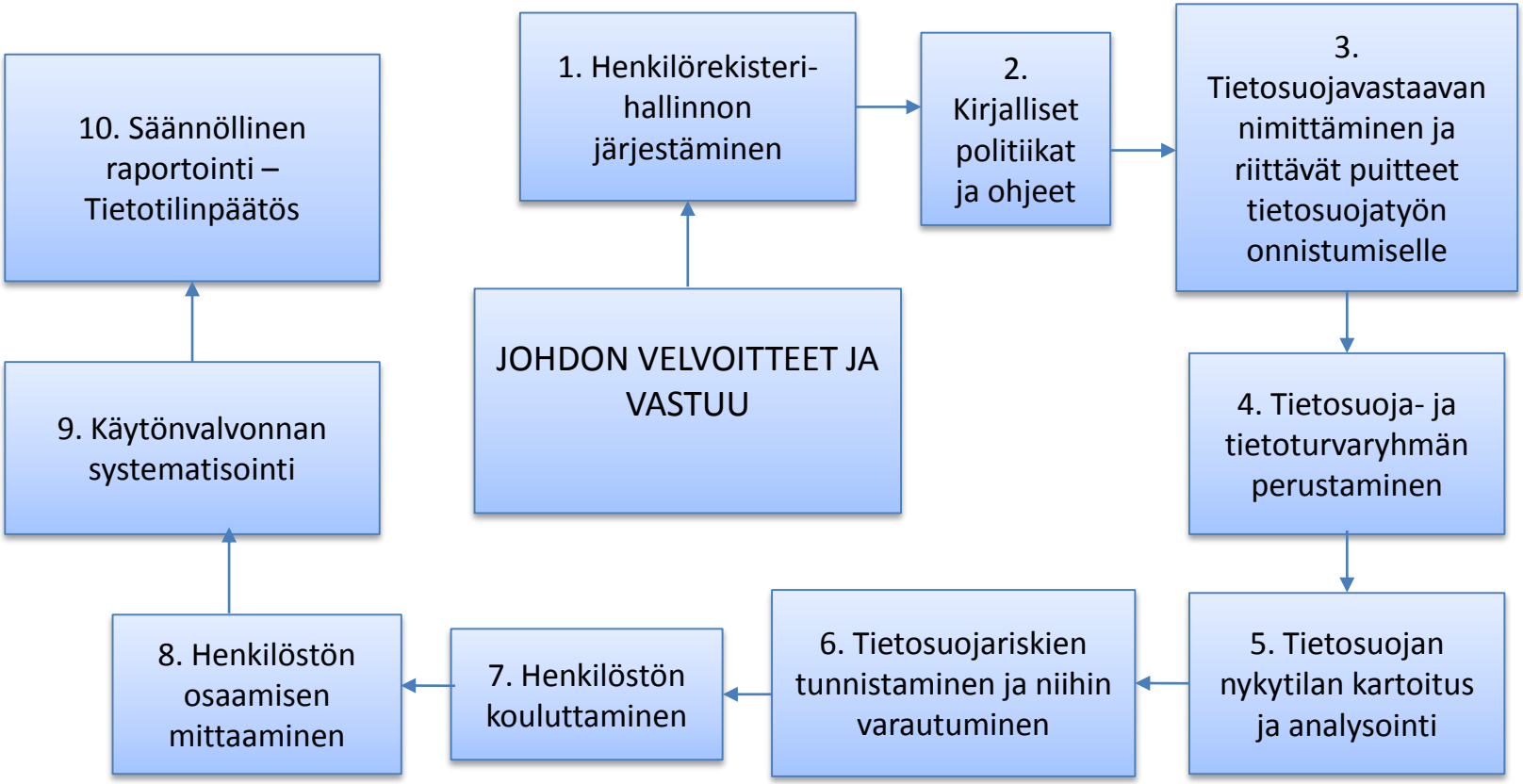
Riskejä GDPR-valmiuden nostossa ja jatkossakin

- Avainhenkilöriskit organisaation sisällä
- EU-tasoiset soveltamisohjeet osin puuttuu
- Uutta lainsäädäntöä tulossa Suomeen (mm. Tietosuojalaki, Tiedonhallintalaki, sote- ja maakuntalakipaketti jne.)
- Paljon uutta terminologiaa kaikille osapuolille
- Sopimusliitteitä tai niiden ehdotuksia alkaa tulemaan ovista ja ikkunoista
- Miten tunnistaa kaikki henkilötietovarannot ja niiden käsittelyprosessit?
- Kansalaiset voivat esittää enemmän tiedusteluja ”Kuka tietojani käsittelee ja miksi?”, ”Haluan tietoni poistettavaksi kaikista järjestelmistä”
- Vakavista tietosuojalaiminlyönneistä tai tietovuodoista voi seurata **tuntuvia seuraamuksia** ml. imagotappioita
- Miten keskittyä oleelliseen?

Mitä kannattaa/pitää tehdä?

- Nimetkää tietosuojavastaava ja antakaa hänen kehittyä osaamisessaan
- Suunnitelkaa tietosuojatyön organisointi huolella
- Toteuttakaa sitä suunnitelman mukaisesti
- Tehkää vaikutustenarviointi suuririskisessä henkilötietojen käsittelyssä (DPIA=Data Protection Impact Assessment)
- Pitäkää tiedon elinkaaren hallinta keskiössä (hävittäkää nyt tarpeeton tieto)
- Muistakaa riittävä dokumentointi
- http://shop.kunnat.net/product_details.php?p=3362 (hyvä julkaisu hankintojen tietosuojaan liittyen)
- Mahdollistakaa henkilöstön osallistua koulutuksiin, jotka liittyvät henkilötietojen käsittelyyn maksutontakin materiaalia on kuten www.arjentietosuoja.fi
- Seuratkaa tietosuovaltuutetun toimiston nettisivuja www.tietosuoja.fi
- Käyttäkää tarvittaessa ulkopuolista apua, jos oma osaaminen eri riitä!

Tietosuojatyön organisointi ja hallinta

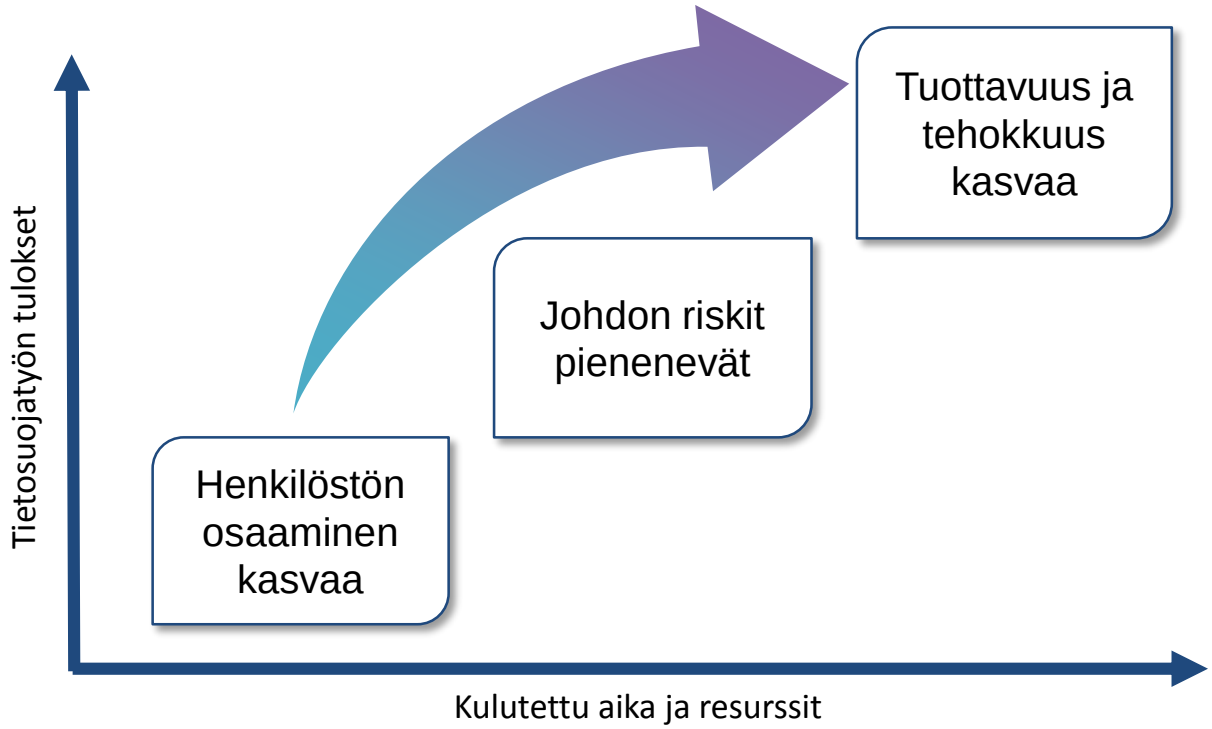


OpiTietosuojaa.fi
Noviisista Mestariksi

Mihin kannattaa keskittyä?

- Nykytila-analyysi ja sen läpikäynti ja tarvittavat korjausliikkeet
- Henkilörekisterihallinnon järjestäminen ja tietosuojaselosteet
- Kirjalliset politiikat, periaatteet ja ohjeet (data protection by design-periaatetta tukeva)
- Teknisen tietoturvan varmistaminen ja varsinkin reagointikyvyn nosto
- Tieto- ja tietojärjestelmäarkkitehtuuri (sekä sen analysointi mitä järjestelmät pitävät sisällään)
- Tiedon elinkaaren hallinta ja tietojen tietoturvaturva
- Käyttövaltuushallinnon läpikäynti
- Riskienhallinta
  - Riskien tunnistaminen ja luokittelu
  - Riskianalyysit ml. DPIA (vaikutusten arviointi)
  - Toimintaohjeet riskien toteutuessa
  - Kirjalliset sopimukset palveluja ostettaessa (turvallisuusliitteet, raportointivelvoitteet, GDPR-liite)
- Seuraamuskäytännöt tietoturva- ja tietosuojarikkomuksissa
- Tietosuojattavan jätteen hävitysprosessin järjestäminen ja valvonta
- Tietoturvan ja tietosuojan omavalvontasuunnitelma
- Tietotilinpäätös (”accountability”-periaatetta tukeva)

Tietosuojatyön tekeminen kannattaa!



OpiTietosuojaa.fi
Noviisista Mestariksi