Tietotilinpäätös 2023

SISÄLLYSLUETTELO

SISÄLLYSLUETTELO 2
JOHDANTO 3
TIETOSUOJAN TOTEUTTAMINEN 4
TIETOSUOJAPERIAATTEET 4
TIETOSUOJAORGANISAATIO 2023 5
TIETOSUOJAOHJEET 6
TIETOSUOJAOHJEET V. 2023 6
TIETOSUOJAKOULUTUKSET 2022 JA 2023 7
TIETOSUOJA HANKINNOISSA 8
TIETOSUOJARISKIEN HALLINTA 8
VAIKUTUSTENARVIOINNIT 9
HENKILÖTIETOJEN TIETOTURVALOUKKAUKSET 10
TIETOSUOJA KUNTALAISEN NÄKÖKULMASTA 12
REKISTERÖIDYN OIKEUKSIIN LIITTYVÄT PYYNNÖT 13
MISTÄ HENKILÖTIEDOT SAADAAN JA MIHIN NIITÄ SIIRRETÄÄN? 13
TIETOPYYNNÖT 13
TIETOSUOJATYÖN TAVOITTEET 2024 14

JOHDANTO

Tietotilinpäätös on osa tietosuojan toteutumisen seurantaa ja EU:n yleisen tietosuoja-asetuksen määrittelemää osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.

Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Tietotilinpäätös on tärkeä osa tätä dokumentointia ja se toimii myös sisäisen ja ulkoisen valvonnan raporttina.

Tietotilinpäätös tarjoaa ajantasaisen tilannekuvan organisaation henkilötietojen käsittelyn nykytilasta ja arvion tietosuojan toteutumisen tasosta. Tietotilinpäätöksessä kartoitetaan myös henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä.

Kehikon tietosuojatyölle kunnassa antaa EU:n tietosuoja-asetus (GDPR). Kansallinen tietosuojalaki täsmentää ja täydentää EU:n tietosuoja-asetusta. GDPR:ää pidetään osin tulkinnanvaraisena asetuksena, minkä vuoksi sen soveltaminen on paikoitellen haastavaa ja oikeuskäytäntö sitä koskien tarkentuu ajan saatossa.

Onnistunut tietosuojatyö vaatii jatkuvaa seurantaa ja kehitystyötä. Tietosuoja on joka tapauksessa kuntaorganisaatiossa läpileikkaava elementti, joka tulee ottaa huomioon jokaisella toimialueella kaikessa henkilötietojen käsittelyssä.

Tuusulan kunta laatii tietotilinpäätöksen pääsääntöisesti vuosittain. Vuonna 2022 ja 2023 on tapahtunut paljon muutoksia tietotilinpäätöksen vastuuhenkilöiden osalta. Vuoden 2022 tietotilinpäätöstä ei laadittu. Tähän tietotilinpäätökseen on koottu tietosuojaa koskeva tietoa pääasiassa vuodelta 2023, mutta osin myös vuodelta 2022.

TIETOSUOJAN TOTEUTTAMINEN

Tietosuoja-asetuksen mukaan rekisterinpitäjä, eli Tuusulan kunta, on vastuussa omien henkilötietoja sisältävien tietovarantojensa osalta tietosuoja-asetuksen vaatimusten mukaisesta käsittelystä. Vaatimustenmukainen käsittely toteutetaan tarvittavin teknisin ja organisatorisin toimenpitein, joilla tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeita ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, sekä teknisempiä toimenpiteitä, kuten monivaiheista kirjautumista ja tietojen elinkaarenhallintaa.

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Rekisterinpitäjällä tarkoitetaan ihmistä tai organisaatiota, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Henkilötietojen käsittelijä on puolestaan ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi IT-palveluntarjoaja, jolla on pääsy rekisterinpitäjän henkilötietoihin.

Henkilötietojen käsittely tarkoittaa kaikkia henkilötietoihin kohdistuvia toimenpiteitä, joita henkilötietoon kohdistuu. Käsittelyä on esimerkiksi henkilötietojen kerääminen, säilyttäminen, käyttö, siirto ja luovuttaminen.

Tietosuoja-asetuksen mukaisia tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat, kun henkilötietoja käsitellään.

TIETOSUOJAPERIAATTEET

- Henkilötietoja on käsiteltävä asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.
- Henkilötietoa on kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten.
- Henkilötietoja on kerättävä vain tarpeellinen määrä käsittelyn tarkoitukseen nähden.
- Henkilötietoja on päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä.
- Henkilötietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.
- Henkilötietoja on käsiteltävä luottamuksellisesti ja turvallisesti.

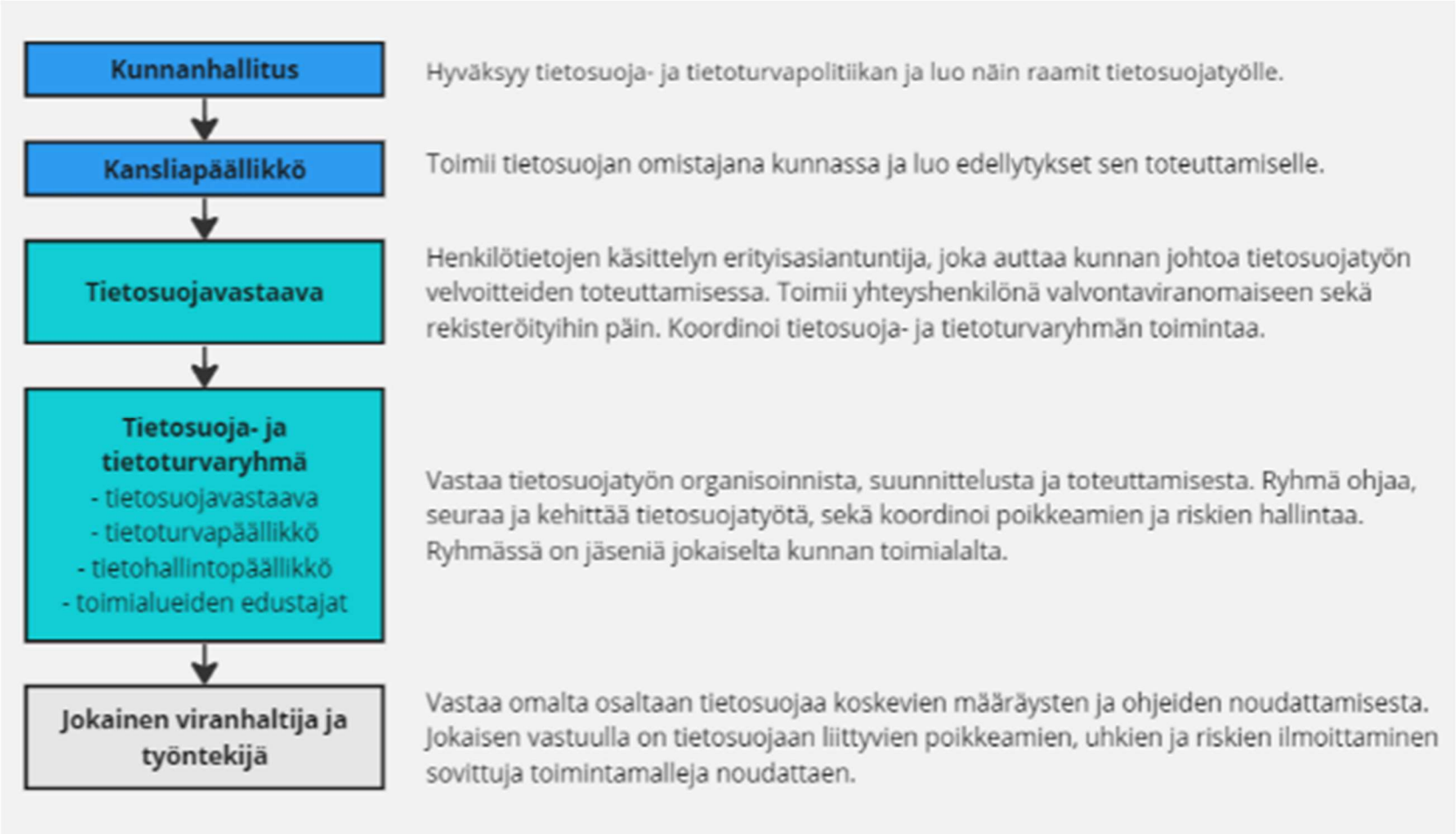
Tietotilinpäätöksen tavoitteena on lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita.

Tietosuojan kansallisena valvontaviranomaisena toimii tietosuojavaltuutetun toimisto. Myös tietosuojatietoisuuden edistäminen, tietosuojaa koskevat selvitykset ja tarkastukset ja rikkomuksista seuraavien hallinnollisten seuraamuksien määrittely kuuluu tietosuojavaltuutetun toimiston tehtäviin.

Kunnan yhteyshenkilönä tietosuojavaltuutetun toimistoon päin toimii tietosuojavastaava. Tavallisimmin tietosuojavastaavan toimistoon ollaan yhteydessä, jos kunnassa tapahtuu tietoturvaloukkaus, joka aiheuttaa riskin rekisteröidylle.

TIETOSUOJAORGANISAATIO 2023

Tietosuojaan tulee kiinnittää huomiota läpi koko organisaation. Ylin johto on viime kädessä vastuussa tietosuojan toteutumisesta, sen toteuttamistavoista ja toteutumisen seurannasta. Tietosuojavastaava neuvoo ja kouluttaa tarvittaessa, koordinoi tietosuojatyötä sekä toimii yhteyshenkilönä viranomaiseen päin. Kuvassa 1 on kuvattu Tuusulan tietosuojatyön organisointitapa vuonna 2023.



Kuva 1 Tietosuojaorganisaatio Tuusulan kunnassa v. 2023

TIETOSUOJAOHJEET

Jokaisen Tuusulan tietojärjestelmiä käyttävän työntekijän, luottamushenkilön tai kolmannen osapuolen henkilön tulee allekirjoittaa tietosuoja- ja tietoturvasitoumus ennen työn aloittamista.

Tuusulan tietosuoja- ja tietoturvapolitiikka on ylimmän johdon hyväksymä asiakirja, joka määrittelee kunnan tietosuojatoiminnan tason ja menettelytavat. Politiikka koskee koko henkilöstöä ja se tulisi katselmoida vuosittain.

Tietosuojaa ja tietoturvaa käsitteleviä ohjeita on lukuisia aina sähköpostin tietoturvallisesta käytöstä henkilötietojen käsittelyn yleisohjeeseen. Jokaisen kunnan työntekijän tulee perehtyä tietosuojaa koskeviin ohjeisiin.

Tuusulan kunnan tietosuojaan liittyviä ohjeita ja lomakepohjia ylläpidetään intranetissä, Työn tueksi -osiossa, jossa ne ovat koko henkilöstön luettavissa. Tietoturva ja tietosuoja -intrasivulta löytyy myös helpot ohjeet tietoturvaloukkauksen asianmukaiseen ilmoittamiseen sekä tietosuojavastaavan, tietohallintopäällikön ja tietoturvapäällikön yhteystiedot opastusta ja kysymyksiä varten.

Tietosuojaan ja tietoturvaan liittyvän ohjeiston koordinoinnista vastaa tietosuojavastaava sekä tietoturvapäällikkö omien vastuualueidensa mukaisesti.

TIETOSUOJAOHJEET V. 2023

Vuonna 2023 käytössä olivat seuraavat ohjeet:

- Tietosuoja- ja tietoturvasitoumus
- Tietosuoja- ja tietoturvapolitiikka
- Henkilötietojen käsittelyn yleisohje
- Ohje tietosuoja- ja tietoturvariskien arvioimiseen ja hallintaan
- Etätyönä tehtävän asiakastyön tietosuojaohje
- Rekisteröityjen informointikäytäntöjä koskeva ohje
- Henkilötietojen tietosuoja- ja tietoturvaloukkauksista ilmoittamisen ohje
- Henkilötietojen tallentaminen ja käsittely O365 -pilvipalveluissa
- Turvakiellon alaisten tietojen käsittelyohje
- Tietopalveluohje
- Sosiaalisen median tietosuojaohje
- Turvapostiohje
- Kyselyiden tietosuojaohje

Tiedonhallintaa, tietosuojaa ja tietoturvaa ohjaavat myös mm. seuraavat sisäiset dokumentit ja aineistot:

- Tiedonhallintamalli
- Tiedonohjaussuunnitelma
- Tietosuojaselostepohja
- Vaikutustenarvioinnin mallipohja
- Tietopyyntöohjeet ja lomakkeet

EU:n tietosuoja-asetuksen ja kansallisen tietosuojalain lisäksi kuntaorganisaation tietosuojatyöhön vaikuttavat useat muutkin lait. Näistä esimerkkeinä esimerkiksi julkisuuslaki, tiedonhallintalaki, opetus- ja koulutusalan tietosuojaa koskevat erityislakinsa, sekä laki sähköisen viestinnän palveluista. Moninaisesta ja muuttuvasta lainsäädännöstä johtuen kunnan tietosuojaohjeistuksen ajan tasalla pitäminen on haastavaa, mutta välttämätöntä.

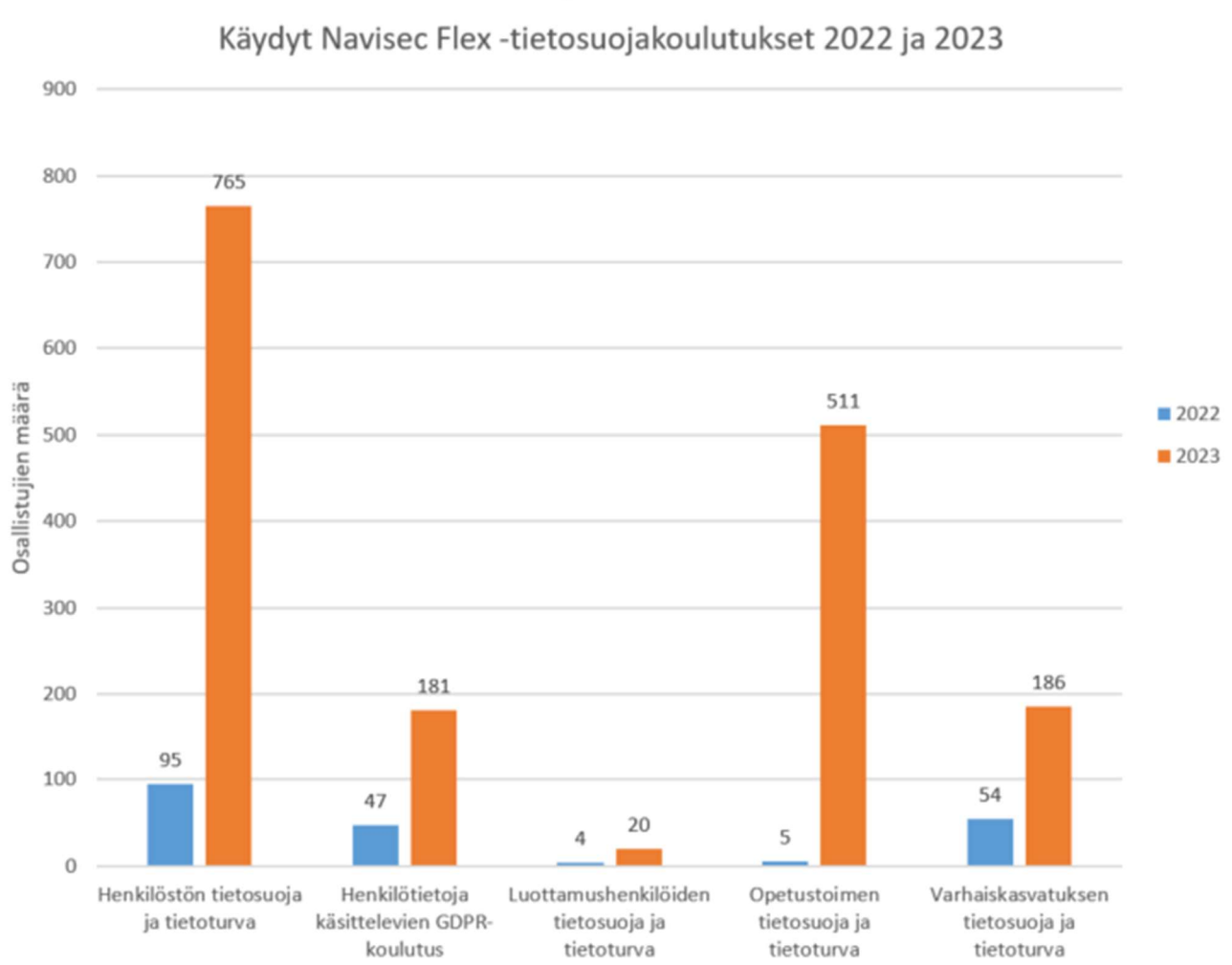
TIETOSUOJAKOULUTUKSET 2022 JA 2023

Voimassaolleen tietosuoja- ja tietoturvapolitiikan mukaan jokainen kunnan henkilöstöön kuuluva on velvollinen suorittamaan itseopiskeluna omaan työtehtäväänsä soveltuvat Navisec Flex -koulutusympäristön kurssit joka toinen vuosi. Esihenkilön vastuulla on seurata alaistensa suorituksia.

Seuraavat opintokokonaisuudet olivat saatavilla v. 2023:

- Henkilöstön tietosuoja ja tietoturva
- Henkilötietoja käsittelevien GDPR-koulutus
- Luottamushenkilöiden tietosuoja ja tietoturva
- Opetustoimen tietosuoja ja tietoturva
- Varhaiskasvatuksen tietosuoja ja tietoturva

Vuonna 2022 oli saatavilla kurssi myös sote-sektorilla toimiville työntekijöille. Hyvinvointialueiden käynnistymisen jälkeen se kuitenkin poistui v. 2023 kurssivalikoimasta. Vuonna 2023 kurssien suoritusmäärät nousivat selkeästi verrattuna vuoteen 2022. Suoritusmäärät jäävät kuitenkin alle ko. tehtäviä suorittavien työntekijöiden määrän, joten koulutuksista informoimista ja koulutusmerkintöjen seuraamista on syytä tehostaa tulevina vuosina. Vuonna 2023 järjestettiin koko kunnan henkilöstölle myös Fiksua tietoturvaa -koulutus Digikuun asiantuntijoiden pitämänä. Koulutuksessa annettiin vinkkejä tietoturvallisen työskentelyn toteuttamiseksi ja käsiteltiin mm. yleisimpiä tietoturvauhkia.



Kuva 2: Navisec Flex -koulutusympäristössä 2022 ja 2023 suoritetut tietosuojakurssit

TIETOSUOJA HANKINNOISSA

Tietosuoja-asetus asettaa velvoitteita hankintojen sopimusehdoille, kun hankinnan seurauksena joku muu alkaa käsitellä henkilötietoja rekisterinpitäjän puolesta. Henkilötietojen käsittelystä on tällöin tehtävä sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välille. Asetus säätää sopimisvelvoitteen lisäksi tietosuojaa koskevan sopimuksen minimisisällöstä, eli ne seikat, joista ainakin tulee sopia.

Sopimuksessa henkilötietojen käsittelystä rekisterinpitäjä ja henkilötietojen käsittelijä sopivat, miten käsittelijän tulee suojata rekisterinpitäjän sille luovuttamat henkilötiedot. On erittäin tärkeää, että Tuusulan kunnan tekemissä henkilötietojen käsittelyä sisältävissä sopimuksissa on liitteenä asianmukainen tietosuojasopimus, jossa kaikki tarvittavat tietosuojanäkökohdat on huomioitu.

Tuusulan kunnalla on intranetissä, Tietosuojaliite-kansiossa, tarvittavat asiakirjapohjat tietosuojasopimuksen tekoa varten. Tärkein niistä on tietosuojaliite, joka tulee aina löytyä sopimuksesta, joka sisältää henkilötietojen käsittelyä palveluntarjoajan lukuun. Palveluntarjoajan toimittamaa tietosuojaliitettä ei tule hyväksyä ilman juristin ja tietosuojavastaavan konsultointia.

Tietosuojaliitteen lisäksi sopimukseen on hyvä liittää myös henkilötietojen käsittelyn ohje sekä henkilötietojen käsittelytoimien kuvaus, jotka löytyvät samasta kansiosta kuin tietosuojaliitteen pohja. Henkilötietojen käsittelytoimien kuvaus on dokumentti, joka tulee toimittaa palvelutarjoajan täytettäväksi hyvissä ajoin ennen sopimuksen allekirjoittamista. Dokumentissa palveluntarjoaja kuvaa omia käytäntöjään ja tiedon suojauksen toimintamallejaan henkilötietojen osalta.

TIETOSUOJARISKIEN HALLINTA

EU:n yleinen tietosuoja-asetus edellyttää rekisterinpitäjältä riskilähtöistä toimintamallia, jossa henkilötietojen käsittelyn riskejä arvioidaan säännöllisesti ja tehdään tarvittavat korjaavat toimenpiteet, mikäli tunnistetaan sellaisia riskejä, joita ei hyväksytä sellaisenaan.

Tietosuoja- ja tietoturvariskien hallintaprosessi koostuu riskien arvioinnista, niiden käsittelystä ja vaikutusten tunnistamisesta, riskien pienentämisestä tai sietämisestä, tarvittavista toimenpiteistä ja riskien seurannasta. Henkilötietojen käsittelyyn liittyvien riskien arviointi on tehtävä lähtökohtaisesti rekisteröityyn kohdistuvien riskien näkökulmasta.

Tuusulan kunnassa käytössä olevassa tietosuojariskien arvioinnin prosessissa henkilötietoon sisältyvän tietosuojariskin suuruutta pyritään ensin arvioimaan asteikolla *ei riskiä - normaali - korkea*. Ensiarvio tehdään Henkilötietojen käsittelyn alkukartoitus -lomakkeella. Kyselyn tulosten perusteella valitaan sopiva työkalu arvioinnin jatkamiseksi.

Jos alkukartoituksessa todetaan, että henkilötietojen käsittelyyn ei sisälly mitään riskiä (eli henkilötietoja ei käytännössä käsitellä), ei tarvita enempää tietosuojatoimenpiteitä. Jos riskitaso on normaali, riittää perustason riskiarvion tekeminen. Mikäli perustason tietosuoja-arvion pohjalta havaitaan korkeaan riskitasoon viittaavia tekijöitä, kuten laajamittaista arkaluonteisten henkilötietojen käsittelyä, on tarve laa-

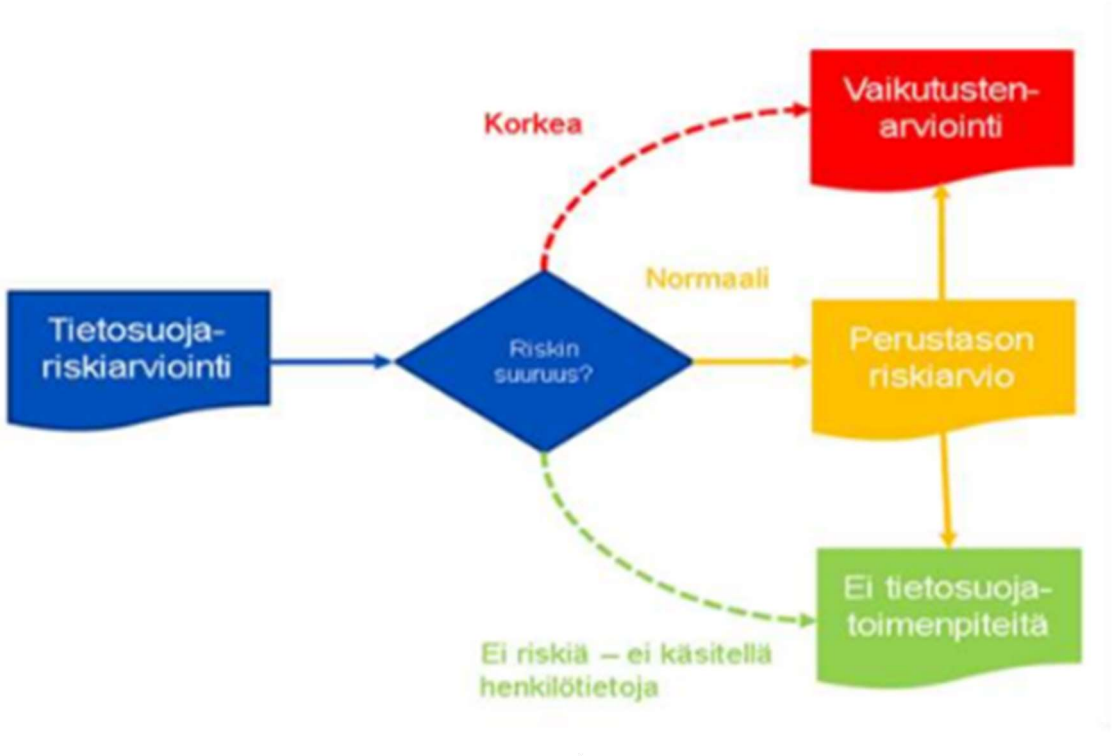
jemmalle vaikutustenarvioinnille tunnistettu. Tuusulan kunnan tietosuojariskien arviointimalli on kuvattu kuvassa 3.

VAIKUTUSTENARVIOINNIT

Vaikutustenarviointi on tärkeä työkalu, jolla varmistetaan, että tietosuoja henkilötietojen käsittelyssä toteutuu GDPR:n mukaisesti.

Kun henkilötietojen käsittelyn alkukartoitus osoittaa, että henkilötietoihin kohdistuu syystä tai toisesta korkea riski, on seuraavaksi tehtävä vaikutustenarviointi. Vaikutustenarviointiprosessi on kuvattu kuvassa 4.

Vaikutustenarviointi toteutetaan työpajatoteutuksella, johon osallistuvat esimerkiksi hankinnasta tai projektista vastaava taho, tietosuojavastaava sekä muut oleelliset tahot, jotka henkilötietojen käsittelyprosessiin kytkeytyvät. Työpajat voidaan järjestää joko ulkopuolisen palveluntarjoajan toimesta tehtyinä, tai sisäisenä toteutuksena. Intranetin tietosuoja-osiossa on lomakepohja vaikutustenarvioinnin suorittamiselle, jota käytetään vaikutustenarvioinnin sisäisessä toteutuksessa.



Kuva 3 Tietosuojariskien arviointimalli

Työpajoissa pyritään tunnistamaan henkilötietojen käsittelyn riskejä sekä riskien suuruuksia. Työpajojen jälkeen laaditaan havaituista riskeistä listaus, sovitaan riskien käsittelytavat, vastuuhenkilöt sekä aikataulu sovituille toimenpiteille. Sen jälkeen tietosuojavastaava hyväksyy vaikutustenarvioinnin. Tärkeää on, että sovittujen toimenpiteiden toteutumista seurataan ja toteutumisen jälkeen tehdään uusi riskiarvio. Näin saadaan selville jäännösriskien suuruus ja tehdään johtopäätökset siitä, ovatko riskit toimenpiteiden jälkeen sillä tasolla, että henkilötietojen käsittely voi alkaa tai jatkua.

Jos vaikutustenarviointi osoittaa, että käsittely aiheuttaa korkean riskin rekisteröidylle, eivätkä tehdyt toimenpiteet ole riittäviä, toteutetaan ennakkokuuleminen.

Ennakkokuulemista koskeva pyyntö toimitetaan tietosuojaviranomaiselle ja sen laatii kunnan tietosuojavastaava.

Kuva 4 Tietosuojan vaikutustenarvioinnin prosessi (Lähde: Tietosuojavaltuutetun toimisto

Vuonna 2023 vaikutustenarviointeja tehtiin seuraaville järjestelmille:

- Microsoftin M365-pilvipalvelu
- Google pilvipalvelut
- Koha Suomi -asiakastietojärjestelmä Keski-Uudenmaan kirjastoverkkoon
- Tuusulan kunnan sisäinen ilmoituskanava
- VIRHO - edunvalvonnan asiakastietojärjestelmä
- Digiasioinnin portaali

Vaikutustenarvioinnit eivät tuoneet esiin sellaista rekisteröityihin kohdistuvaa riskitasoa, joka olisi estänyt järjestelmän käyttöönottoa tai käytön jatkamista. Jäännösriskien suuruudet ja vaikutustenarviointien perusteella tehdyt toimenpiteet ovat jääneet osittain dokumentoimatta, mikä on selkeä kehityskohde tulevalle vuodelle.

HENKILÖTIETOJEN TIETOTURVALOUKKAUKSET

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jossa henkilötietoja katoaa, muuttuu, tai niihin pääsee käsiksi tahoja, joilla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaukset voivat tapahtua tahallisesti tai vahingossa. Tyypillisiä henkilötietojen tietoturvaloukkauksia Tuusulan kunnassa ovat lähivuosina olleet tietojen lähettäminen epähuomiossa väärälle henkilölle, tietojen näkyminen laajemmalle henkilömäärälle kuin on tarkoitus, tai tietojenkalastelun seurauksena tapahtunut tietovuoto. Tietoturvaloukkauksesta voi seurata esimerkiksi identiteettivarkaus, mainehaitta, tai salassapitovelvollisuuden alaisen henkilötiedon paljastuminen.

Tuusulan kunta ohjeistaa työntekijöitään ilmoittamaan tietoturvapoikkeamista intranetistä löytyvien ohjeiden avulla. Tuusulalla on käytössä WPro-järjestelmä, jonne on tarkoitus kirjata eri väyliä pitkin tulleet ilmoitukset tietoturvapoikkeamista. Ilmoituksia tulee tyypillisesti suoraan WPro:n kirjattuna, sähköpostitse ja puhelimitse.

Seuraavan sivun kuva kertoo WPro-järjestelmään ja/tai asianhallintajärjestelmä CaseM:n kirjatut ilmoitukset tietoturvapoikkeamista vuosina 2022 ja 2023.

Kirjaamiskäytännöissä on tunnistettu olevan tällä hetkellä puutteita, sillä osa ilmoituksista jää kirjaamatta WPro-järjestelmään. Tästä johtuen todelliset lukumäärät saattavat poiketa taulukon luvuista. Ilmoitus tietoturvaloukkauksesta tehdään mata-

lalla kynnyksellä. Ilmoituksia saapuu tietosuojavastaavalle, tietoturvapäällikölle sekä tietohallintopäällikölle.

Ilmoituksen saapumisen jälkeen arvioidaan, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille. Riskin taso määrittää toimenpiteet, joihin rekisterinpitäjä ryhtyy.

Mikäli loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille, täytyy siitä ilmoittaa valvontaviranomaiselle, eli tietosuojavaltuutetun toimistoon. Jos loukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidyn oikeuksille ja vapauksille, tulee siitä ilmoittaa myös suoraan rekisteröidylle.

Kuva 5 Tietoturvaloukkausilmoitukset v. 2022-2023

Vuonna 2022 kynnyksen tietoturvapoikkeaman ilmoittamisesta tietosuojavaltuutetulle ylitti yksi ilmoitus. Siinä henkilötietojen käsittelijän järjestelmävirheen seurauksena henkilötietoja päätyi väärälle vastaanottajalle.

Vuonna 2023 tietosuojavaltuutetun toimistoon ilmoitettiin kolmesta tietoturvapoikkeamasta. Kahdessa tapauksessa kyse oli kunnan sisäisestä inhimillisestä erehdyksestä. Yksi poikkeama johtui laajamittaisesta tietojenkalastelusta. Tietojenkalastelukampanjat ovat yleistyneet viime vuosina ja niihin tulee varautua myös jatkossa. Kalastelu saattaa johtaa laajamittaiseenkin tietovuotoon, jossa arkaluontoisia tietoja päätyy verkkorikollisten käsiin.

Inhimillisten virheiden seurauksena tapahtuviin tietoturvapoikkeamiin voidaan vastata lisäämällä koulutusta, sekä muuttamalla järjestelmien oletusasetuksia siten, että epähuomiossa tehdyt virheet ovat epätodennäköisempiä.

Tietojenkalasteluun pystytään varautumaan lisäkoulutuksella, jolloin kalastelun kohteeksi joutuneet henkilöt tunnistavat kalasteluyritykset paremmin. Osansa kalastelukampanjoiden torjunnalla on myös tek-

nisellä varautumisella ja jatkuvalla tietoturvallisuuden parantamisella. Tällä hetkellä Tuusulassa on käytössä tietoturvallisuuteen liittyvien poikkeamien havainnointipalvelu ulkopuolisen toimijan toimesta toteutettuna.

TIETOSUOJA KUNTALAISEN NÄKÖKULMASTA

Rekisterinpitäjä on velvollinen toimittamaan rekisteröidyille henkilötietojen käsittelyä koskevia tietoja. Tiedot on annettava tiiviissä, läpinäkyvässä ja helposti ymmärrettävässä muodossa. Rekisterinpitäjän on lisäksi helpotettava rekisteröidyn oikeuksien toteuttamista ohjeistamalla ja luomalla toimintamallit oikeuksien toteutumiselle.

Tuusulan kunta antaa tarvittavan informaation henkilötietojen käsittelystä kunnan internetsivulla. Sivulla kuvataan Tuusulan kunnan tapaa käsitellä henkilötietoja, sekä ohjataan rekisteröidyn oikeuksista kertovalle sivulle. Lisäksi sivuilla on rekisteriselosteet, joissa kerrotaan henkilötietojen käsittelystä tarkemmin.

Tuusulan kunta kerää henkilötietoja eri rekistereihin. Jokaisesta rekisteristä löytyy julkisesti seuraavat tiedot:

- rekisterin nimi
- rekisterinpitäjän ja tämän edustajan yhteystiedot
- rekisteriasioiden yhteyshenkilö
- tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset
- rekisterin tietosisältö
- tieto henkilötietojen säännönmukaisista luovutuksista
- henkilötietojen säilytysaika, tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- rekisterin ylläpitojärjestelmät ja suojauksen periaatteet
- rekisteröidyn oikeus saada pääsy tietoihin
- oikeus tiedon oikaisemiseen
- muut oikeudet

Rekisteriselosteiden laatimisesta huolehtivat toimialojen vastuuhenkilöt. Tietosuojavastaavalta saa neuvoja tarpeen mukaan rekisteriselosteen laadintaan.

Jokaiselle rekisterille on nimetty vastuuhenkilö, joka vastaa omalta osaltaan kysei-

sen rekisterin tietosuojasta, rekisteriselosteen lainmukaisuudesta, rekisteröityjen tietopyyntöihin vastaamisesta ja muiden rekisteröityjen oikeuksien toteuttamisesta.

REKISTERÖIDYN OIKEUKSIIN LIITTYVÄT PYYNNÖT

Rekisteröidyillä on erilaisia oikeuksia liittyen omiin henkilötietoihinsa ja niiden hallintaan. Rekisteröidyn oikeuksiin lukeutuvat:

- saada tietoja henkilötietojensa käsittelystä
- saada tutustua tietoihin
- oikeus tietojen oikaisemiseen
- oikeus tietojen poistamiseen
- oikeus käsittelyn rajoittamiseen
- oikeus vastustaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröidyn oikeuksia sovelletaan eri tavoin riippuen siitä, mikä on ollut henkilötietojen käsittelyn oikeusperuste. Jos oikeusperuste on esimerkiksi lakisääteinen, ei oikeutta tietojen poistamiseen voi aina soveltaa.

Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien toteutumista. Tuusulan kunnalla on erillinen verkkosivu rekisteröidyn oikeuksille. Siellä kerrotaan mitä oikeuksia rekisteröidyllä on ja miten niitä voi toteuttaa.

Pääsääntöisesti GDPR:n mukaisia rekisteröityjen oikeuksia voi toteuttaa Tuusulassa täyttämällä verkkosivulta löytyvän sähköisen lomakkeen, tai toimittamalla lomakkeen TuusInfon palvelupisteeseen. Sähköisen lomakkeen käyttäminen vaatii vahvaa tunnistautumista. Paperiversion toimittamisen yhteydessä tulee myös varautua todistamaan henkilöllisyytensä.

MISTÄ HENKILÖTIEDOT SAADAAN JA MIHIN NIITÄ SIIRRETÄÄN?

Tuusulan kunnan henkilöstön sekä kuntalaisten henkilötiedot saadaan pääsääntöisesti rekisteröidyiltä itseltään tai viranomaiselta. Henkilötietoja voidaan siirtää kunnan sisäisissä järjestelmissä järjestelmästä toiseen, jos käyttötarkoitus pysyy samana. Sekä kunnan työntekijöiden, että kuntalaisten siirretään toisille rekisterinpitäjille ainoastaan rekisteröidyn suostumuksella tai lainsäädäntöön perustuen.

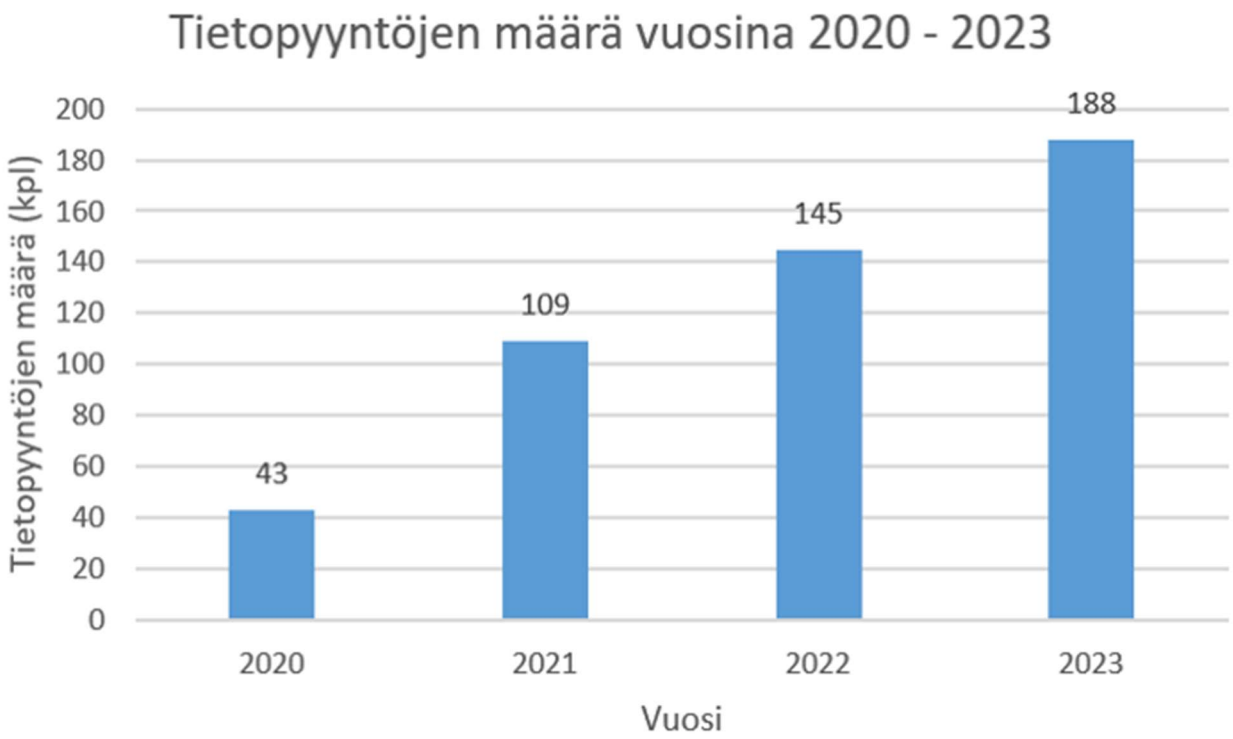
Tuusulan kunta ei lähtökohtaisesti siirrä keräämiään henkilötietoja EU/ETA -alueen ulkopuolelle.

TIETOPYYNNÖT

Julkisuuslain mukaan jokaisella on oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tuusulan kunnan asiakirjoja koskevat tietopyynnöt suunnataan asiasta vastaavalle viranhaltijalle tai toimialueelle. Tietopyynnön voi lähettää käyttämällä sähköisen asioinnin lomakkeita, mikä edellyttää vahvaa tunnistautumista.

Tietopyyntöjen määrä on kasvanut tasaisesti viimeisen neljän vuoden aikana.

Seuraavan sivun taulukosta löytyy julkisuuslain perusteella saapuneiden tietopyyntöjen lukumäärä v. 2020 - 2023.



Kuva 6 Tietopyyntöjen määrän kehitys Tuusulan kunnassa v. 2020 - 2023

TIETOSUOJATYÖN TAVOITTEET 2024

Vuonna 2023 toimintaympäristössä on tapahtunut paljon suuria muutoksia. Venäjän hyökkäyssota Ukrainassa on lisännyt jännitteitä ja moninapaisuutta, aiheuttaen tarpeen varautua yhä kasvaviin kyberuhkiin ja hybridivaikuttamisyrityksiin.

Euroopan energiakriisi, korkea inflaatio ja markkinakorkojen nousu ovat rasittaneet niin kuntalaisten kuin kunnan taloutta. Toisaalta tekoälyä hyödyntävät digitaaliset palvelut ovat monipuolistuneet ja yleistyneet nopeasti. Vastuullisuuden vaatimukset kasvavat lisääntyvän sääntelyn muodossa esimerkiksi tekoälyn ja siihen liittyvän tietosuojariskin osalta koko Euroopassa.

Yleinen EU:n tietosuoja-asetus täytti viisi vuotta. Se luo pohjan kaikelle tietosuojatyölle Euroopassa. Vuonna 2023 kirjattiin hallitusohjelmaan hallinnollisen seuraamusmaksun käyttöönotto tietosuojarikkomusten osalta myös julkisella sektorilla. Henkilötietojen siirrot Euroopan ja Yhdysvaltojen välillä ovat helpottuneet komission tekemän riittävyyspäätöksen jälkeen.

Paljon on siis tapahtunut tietosuojan ja tietoturvan osalta vuonna 2023 Euroopassa ja Suomessa. Myös meillä Tuusulassa on syytä pysyä sekä regulaation, että muiden turvallisuusympäristön muutosten mukana.

Tuusulan kunta panostaa tietosuoja- ja tietoturvatyöhön merkittävästi vuonna 2024. Tietosuojatyön osalta kehitämme toimintaamme seuraavasti:

1. Digiturvamallin käyttöönotto

Suurin tietosuojatyötä koskeva uudistus on tietosuojaa, tietoturvaa ja kyberturvaa koskevan hallintajärjestelmän käyttöönotto hyödyntäen Digiturvamalli-sovellusta. Vaatimuskehikkoina järjestelmässä toimivat GDPR, tiedonhallintalaki sekä julkisen hallinnon tietoturvan arviointikriteeristö Julkri. Näiden pohjalta dokumentoimme tiedonhallintamallimme sekä tehostamme

omaa tietosuoja-, tietoturva- ja kyberturvatyötämme lainsäädäntöön perustuen. Digiturvamallilla pyrimme dokumentoimaan asiat systemaattisesti, selkeästi ja yhdenmukaisesti niin, että tarvittava tieto ja dokumentit löytyvät pääsääntöisesti yhdestä paikasta.

2. Riskienhallintaprosessin uudistaminen

Läpikäymme tietosuojariskien hallintamallin. Teemme siihen tarvittavat muutokset ja dokumentoimme jatkossa tietosuojaa koskevan riskienhallintatyön tulokset Digiturvamalliin.

3. Tietosuojakävelyt

Vuonna 2024 toteutetaan tietosuojakävelyitä valituilla palvelualueilla ja auditoidaan näin jokapäiväisen työnteon käytäntöjä tietosuojanäkökulmasta.

4. Tietosuoja- ja tietoturvakoulutusten kartoitus ja koulutuksiin osallistumisen tehostaminen

Läpikäymme markkinoilta löytyviä koulutusohjelmia liittyen tietosuojaan ja tietoturvaan. Valitsemme niistä Tuusulan kunnan työntekijöille sopivimman kokonaisuuden käyttöön. Koska tietosuoja- ja tietoturvakoulutusten suoritusmäärät jäävät tavoitteesta, muistutetaan henkilöstöä koulutusten suorittamisen tärkeydestä. Myös esihenkilöille terävöitetään kurssisuoritusten läpikäyntiä työntekijöiden kanssa käytävissä kehityskeskusteluissa.

5. Vuosikello

Tietosuojatyössä otetaan v. 2024 käyttöön vuosikello, jonka avulla systematisoimme toimintaa esimerkiksi tietosuojaa koskevien päivityskäytäntöjen ja sisäisen valvonnan osalta.

6. Teknisen tietoturvan parantaminen

Tarkastelemme Microsoft-ympäristömme tietoturvaa ja kehitämme sitä edelleen osana jatkuvuudenhallintatyötämme.

Vuoden 2024 tietosuojatyön tavoitteiden toteutumisen kautta saamme jäsenneltyä ja dokumentoitua tietosuojaa ja tietoturvaa koskevaa työtä uudella tavalla. On tärkeää osallistaa koko henkilöstö ottamaan tietosuojaan ja tietoturvaan liittyvät seikat huomioon jokapäiväisessä työssään, sekä tarjota heille tarvittava tieto ja työkalut sitä varten. Myös johdon sitoutuminen ja aktiivinen osallistuminen tietosuojatyöhön on tärkeää, sillä johto viime kädessä vastaa tietosuojaa ja tietoturvaa koskevista linjauksista ja tuloksista.