TIETOTILINPÄÄTÖS 2024

SISÄLLYSLUETTELO

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.

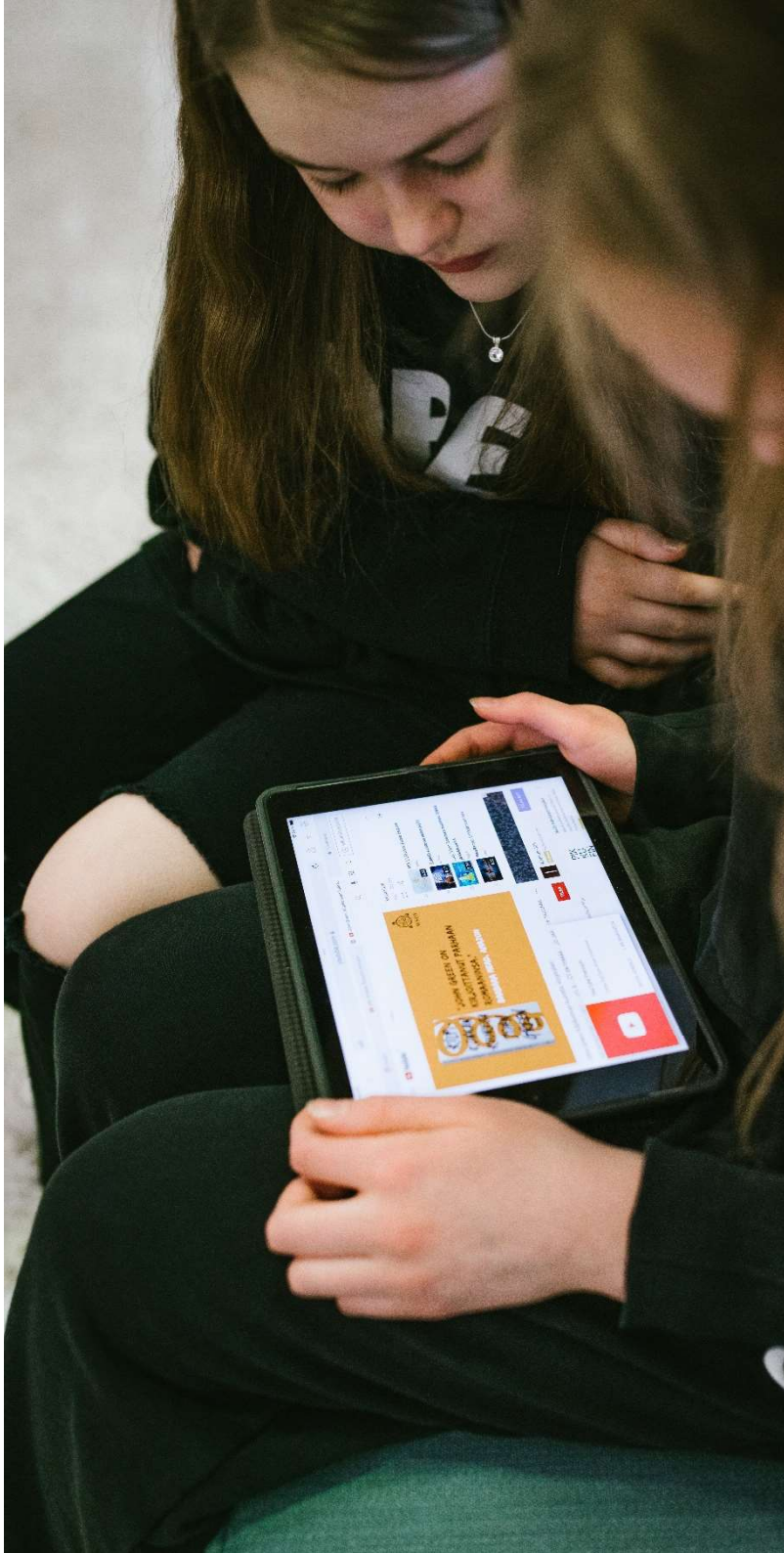
Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Tietotilinpäätös on tärkeä osa tätä dokumentointia ja se toimii myös sisäisen ja ulkoisen valvonnan raporttina.

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. Nykyisen hallitusohjelman puitteissa pyritään edistämään tietosuojaan liittyvien hallinnollisten sakkomaksujen määräämismahdollisuuden ulottamista myös julkisen puolen toimijoihin. Odotettavissa on, että muutos lainsäädäntöön toteutetaan lähivuosien aikana.

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 vuosittain. Tähän tietotilinpäätökseen on koottu tietosuojaa koskeva tietoa vuodelta 2024.



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.

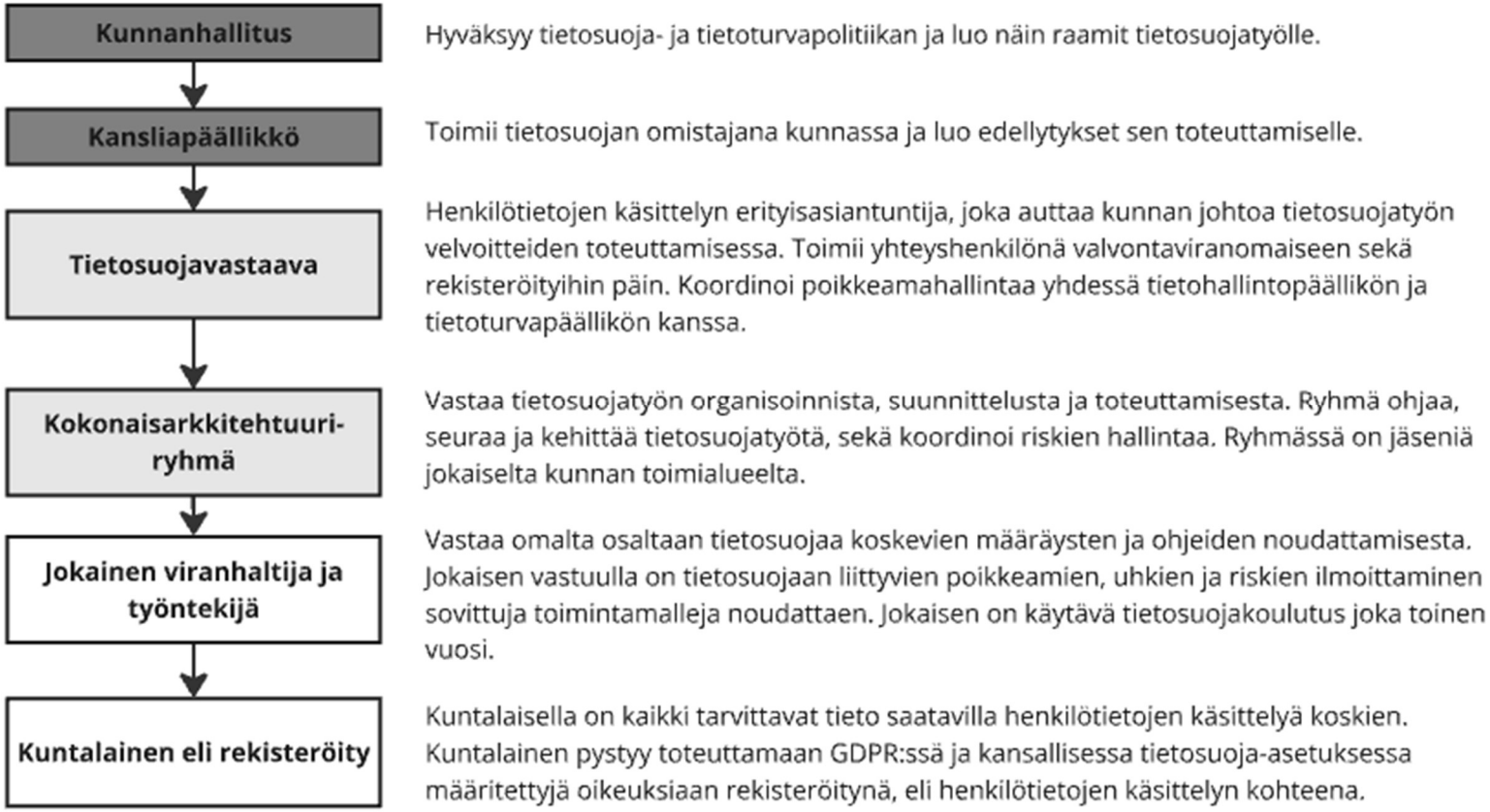
Tietotilinpäätöksen tavoitteena on lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita.

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 2024

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 2024.



Kuva 1 Tietosuojaorganisaatio Tuusulan kunnassa v. 2024

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. 2024

Vuonna 2024 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
- Sosiaalisen median tietosuojaohje
- Turvapostiohje
- Kyselyiden tietosuojaohje
- Ohje luottamushenkilöille koskien tietojen julkisuutta ja salassapitoa
- Ohje tietosuojaselosteiden täyttämiseen
- Ohje henkilötietojen korjaus- ja tarkastuspyyntöjä koskien

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 2023-2024

Voimassaolleen tietosuoja- ja tietoturvapolitiikan mukaan jokainen kunnan henkilöstöön kuuluva on velvollinen suorittamaan itseopiskeluna omaan työtehtäväänsä soveltuvat Navisec Flex -koulutusympäristön kurssit joka toinen vuosi. Työntekijän tulisi suorittaa tarvittavat kurssit koeajan kuluessa.

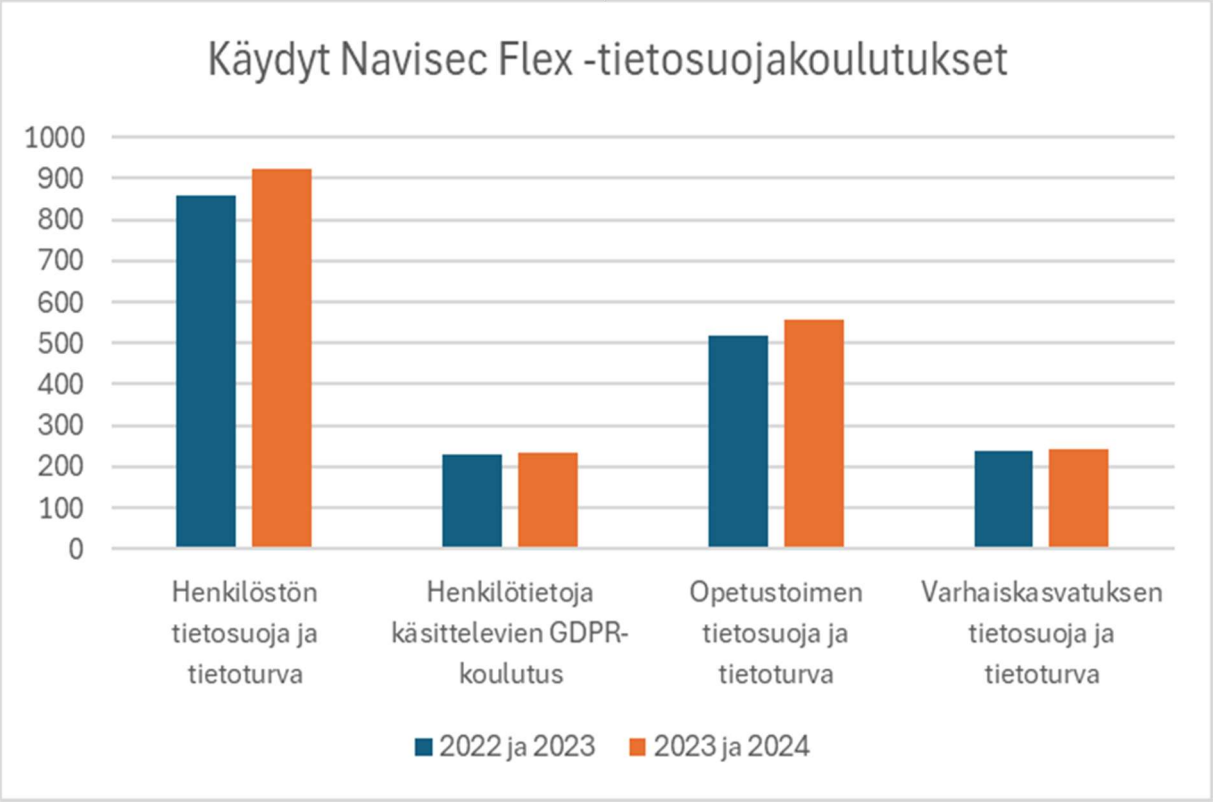
Esihenkilön vastuulla on seurata alaistensa suorituksia ja muistuttaa suoritusten tärkeydestä esimerkiksi kehityskeskusteluiden yhteydessä.

Seuraavat opintokokonaisuudet olivat saatavilla v. 2024:

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

Kuvassa 2 tarkastellaan edellisten kahden vuoden aikajaksojen kurssisuoritusmääriä. Siitä nähdään, että suoritusmäärä on noussut hieman ajanjaksolla 2023-2024 verrattuna vuoden 2022-2023 jaksoon. Suorituksia on kuitenkin merkittävästi vähemmän, kuin työntekijöitä, joten koulutusten tärkeydestä on syytä muistuttaa työntekijöitä jatkossakin.

Vuoden 2025 toukokuussa Navisec Flex -järjestelmä poistuu käytöstä ja tietosuojakurssit löytyvät jatkossa Eduhouse-kurssialustalta. Eduhouse tulee tarjoamaan lisäksi laajan valikoiman tietosuojaan ja tietoturvaan liittyviä syventäviä kursseja, joita työntekijät voivat tulevaisuudessa suorittaa tarpeen mukaan.



Kuva 2: Navisec Flex -koulutusympäristössä suoritetut tietosuojakurssit v. 2022-23 ja 2023-24

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 kunnan lakimiehen 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 intran Tietoturva ja tietosuoja -osion dokumenttipohjista löytyvän riskien alkukartoituslomakkeen avulla. 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. Myös tähän löytyy dokumenttipohja intrasta. Mikäli perustason tietosuoja-arvion pohjalta havaitaan korkeaan riskitasoon

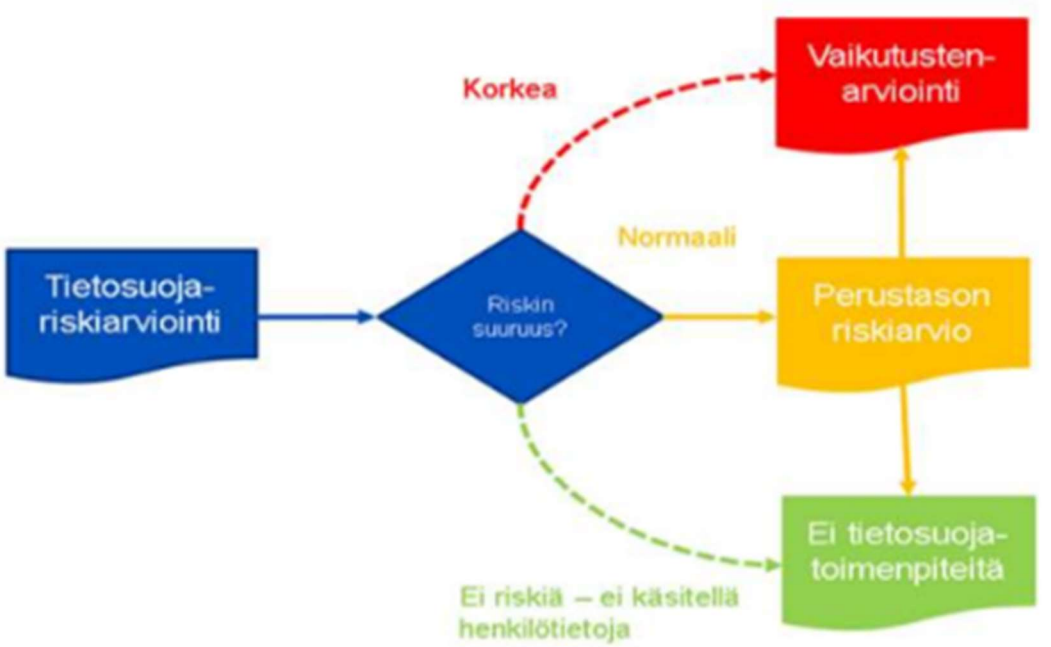
viittaavia tekijöitä, kuten laajamittaista arkaluonteisten henkilötietojen käsittelyä, on tarve laajemmalle vaikutustenarvioinnille tunnistettu. Tuusulan kunnan tietosuojariskien arviointimalli on kuvattu kuvassa 3.

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 2024 vaikutustenarviointeja tehtiin seuraaville järjestelmille:

- Movit-koulukuljetusjärjestelmä
- Tiera City, rakennetun ympäristön toimintojen ja tiedonhallinnan kokonaisjärjestelmä
- Microsoft 365 kouluympäristössä (jatkuu v. 2025)
- Google Workspace for Education (jatkuu v. 2025)
- Visma Inschool / Wilma (jatkuu v. 2025)

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.

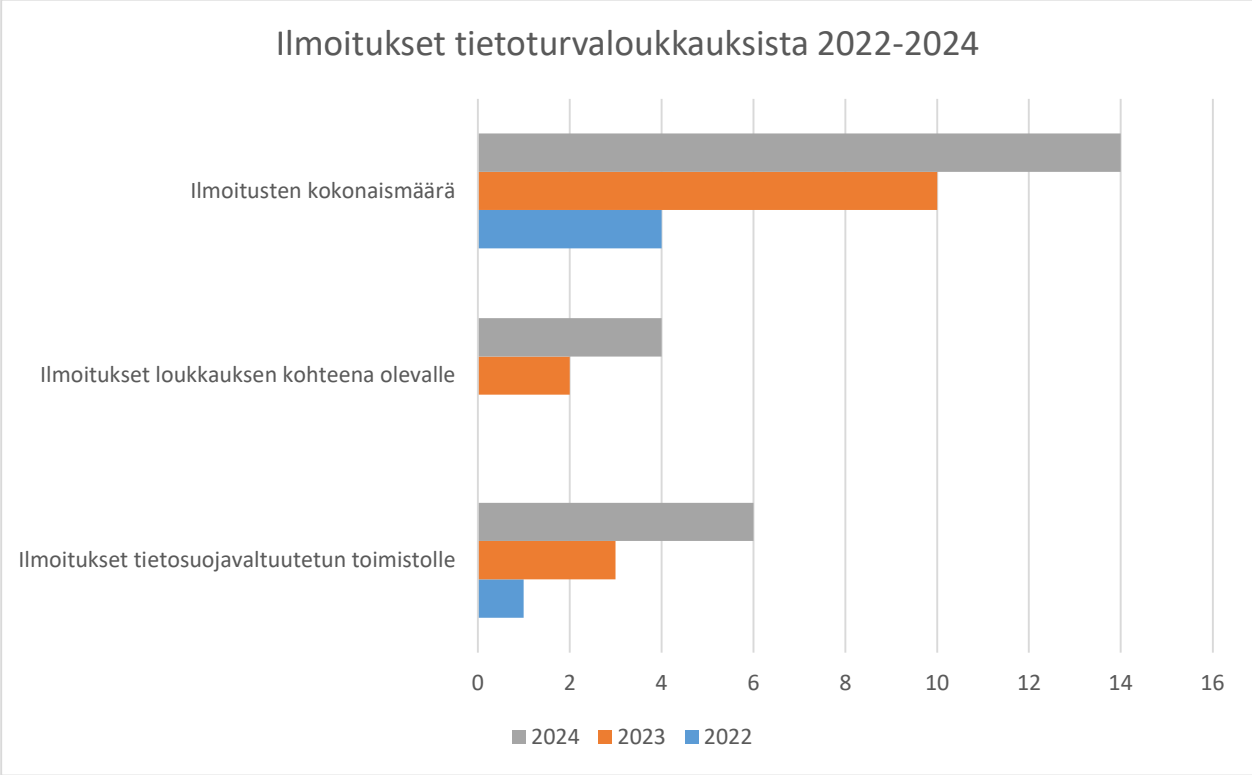
Seuraavan sivun kuva kertoo WPro-järjestelmään ja/tai asianhallintajärjestelmä CaseM:n kirjatut ilmoitukset tietoturvapoikkeamista vuosina 2022, 2023 ja 2024.

Ilmoitus tietoturvaloukkauksesta tulee ohjeistuksen mukaisesti tehdä matalalla kyn-

nyksellä. 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.

Ilmoitusten määrä on kasvanut tasaisesti viime vuosina, kuten kuvasta 5 nähdään. Vuonna 2024 suurin osa poikkeamista johtui inhimillisistä virheistä. Osin loukkausilmoitusten määrän nousu saattaa johtua ilmoituskynnyksen madaltumisesta.



Kuva 5 Tietoturvaloukkausilmoitukset v. 2022-2024

Vuonna 2022 kynnyksen tietoturvapoikkeaman ilmoittamisesta tietosuojavaltuutetulle ylitti yksi ilmoitus. Vuonna 2023 tietosuojavaltuutetun toimistoon ilmoitettiin kolmesta tietoturvapoikkeamasta. Kahdessa tapauksessa kyse oli kunnan sisäisestä inhimillisestä erehdyksestä. Yksi poikkeama johtui laajamittaisesta tietojenkalastelusta.

Vuonna 2024 tietosuojavaltuutetun toimistoon tehtiin kuusi ilmoitusta tietoturvaloukkauksista. Näistä viisi tapahtui sivistyksen toimialueella inhimillisten erehdysten seurauksena. Yksi ilmoitus tehtiin järjestelmätoimittajalla tapahtuneen inhimillisen virheen seurauksena.

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

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

Vuonna 2024 aloitettiin tiedonhallintamallin ylläpitoon hankitun Digiturvamalli-ohjelmiston käyttöönoton valmistelutyö. Toimialueet ovat vieneet omien vastuujärjestelmiensä ja -tietovarantojensa osalta Digiturvamalliin tietoa, jonka avulla saadaan jatkossa tietosuojaselosteet tietovarantokohtaisesti kunnan verkkosivuille ja järjestelmäkohtaiset tietosuojaselosteet poistuvat. Muutos tulee näkyviin kuntalaisille, kun uudet verkkosivut julkaistaan vuoden 2025 alkupuoliskolla.

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.

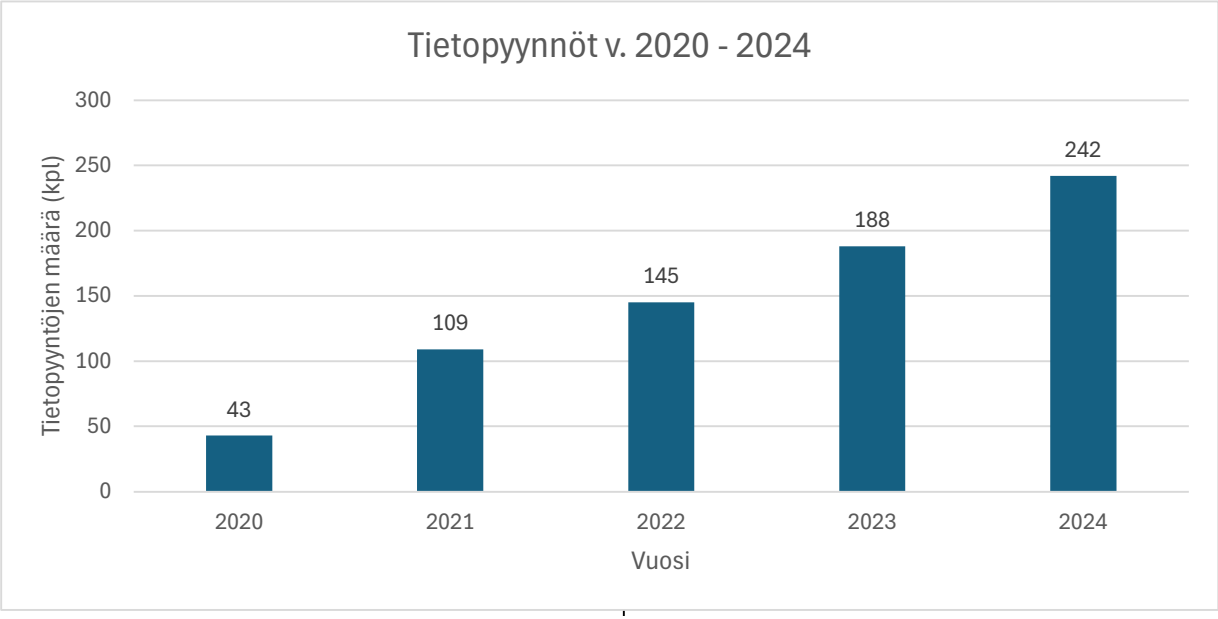
Tuusulan kunta ei lähtökohtaisesti siirrä keräämiään henkilötietoja EU/ETA -alueen ulkopuolelle.

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, kuten tietoturvaloukkausten, määrä on kasvanut tasaisesti viime vuosina.

Seuraavan sivun taulukosta löytyy julkisuuslain perusteella saapuneiden tietopyyntöjen lukumäärä v. 2020 - 2024. Luvut sisältävät kaikki julkisuuslain perusteella tulleet julkisten tai salaisten asiakirjojen tietopyynnöt, sekä GDPR:n mukaiset henkilötietojen tarkastuspyynnöt.



Kuva 6 Tietopyyntöjen määrän kehitys Tuusulan kunnassa v. 2020 - 2024

TIETOSUOJATYÖN KEHITTÄMINEN VUONNA 2024

Vuonna 2024 aloitimme tiedonhallintamallin rakentamisen Digiturvamalli-sovellukseen. Rakentamistyö on vielä kesken vuoden 2024 lopussa. Digiturvamallin ominaisuuksien avulla saamme tietosuojaselosteet muutettua tietovarantokohtaisiksi. Tämä helpottaa kuntalaisia löytämään tietoa halutusta osa-alueesta, pistemäisen henkilötietojen käsittelyn riskin vähentämistä ja tietosuojaselosteiden sisällön hallittua ylläpitämistä. Uudet tietosuojaselosteet tulevat kuntalaisten saataville, kun kunnan verkkosivut uudistuvat vuoden 2025 alkupuoliskolla. Digiturvamallista on saatavilla myös asianmukainen henkilötietojen käsittelytoimien kuvaus, jollaista Tuusulan kunnassa ei ole aiemmin ollut kunnan sisällä saatavilla. Tämä toteutetaan intran uudistustyön ohessa vuoden 2025 aikana.

Tietosuojakävelyitä suoritettiin vuonna 2024 kaksi kappaletta. Toinen kävelyistä suoritettiin koulussa ja toinen kunnan toimistotiloissa Sahankulmassa. Tietosuojakävelyissä ei tullut esiin kriittisiä riskejä, mutta eri tasoisia kehityskohteita löytyi.

Tietosuojakävelyt on koettu hyödyllisiksi, sillä niiden avulla saadaan tietoa tietosuoja-asioiden hallinnasta kunnan eri toimialueilla, havaitaan kehityskohteita toimintatavoissa, mutta ennen kaikkea pystytään auttamaan toimialueita tietosuojaa koskevissa kysymyksissä ja saadaan keskusteluyhteys tietosuojavastaavan ja toimialueiden välillä. Näiden kokemusten perusteella tietosuojakävelyitä on tarkoitus jatkaa myös vuonna 2025.

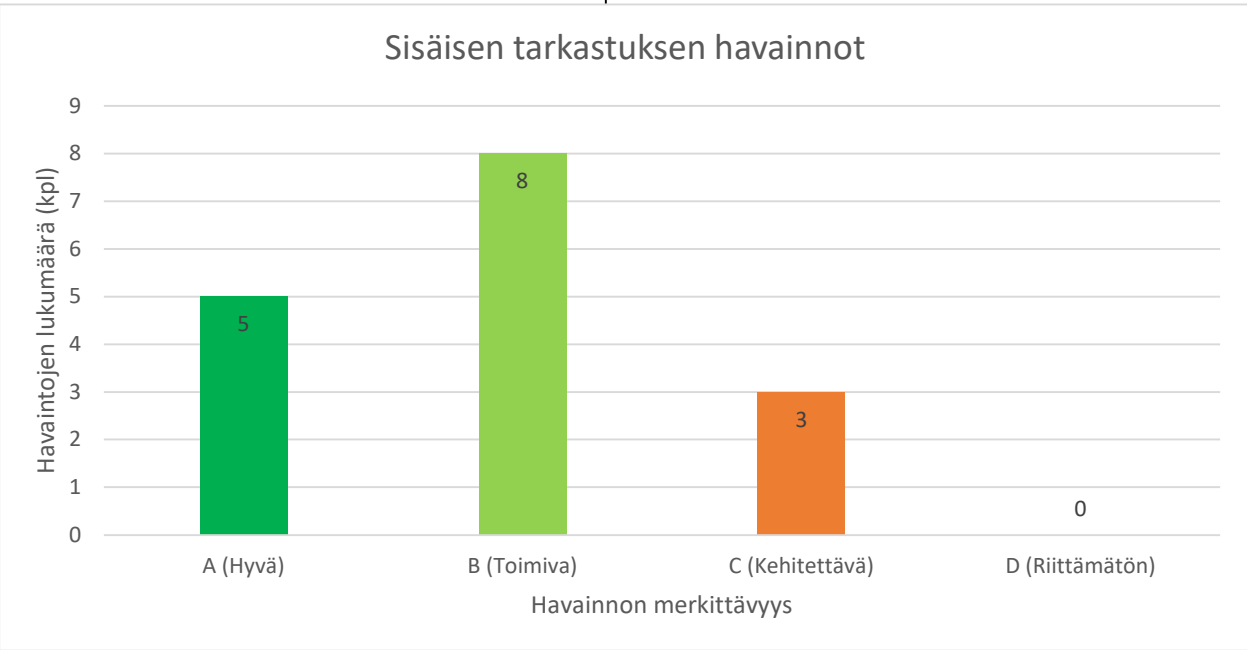
Aiemmin toiminut tietosuoja- ja tietoturvaryhmä lakkautettiin ja tietosuoja-asioiden hallinnointi siirrettiin uudelle kokonaisarkkitehtuuriryhmälle. Samalla otettiin käyttöön arkkitehtuurihyväksyntäprosessi, jonka kautta pyritään varmistamaan uusien tietojärjestelmien, tai nykyisten järjestelmien muutosten, sopivan kunnan kokonaisarkkitehtuuriin ja täyttävän tiedonhallintalakiin ja tietosuoja-asetukseen liittyvät vaatimukse. Samassa yhteydessä on tarkoitus tunnistaa tarve ja toteuttaa mahdolliset

riskiarvioinnit ja tietosuojan vaatimustenarvioinnit hyvissä ajoin ennen tietojärjestelmien käyttöönottoa.

Vuonna 2024 kartoitettiin tarjolla olevia tietosuoja- ja tietoturvakoulutusjärjestelmiä. Navisec Flex -järjestelmästä päätettiin luopua ja sopimus irtisanottiin loppumaan toukokuun 2025 loppuun.

Sisäisen tarkastuksen suorittanut BDO teki tarkastuksen yhteydessä havaintoja ja luokitteli ne merkittävyyden mukaan asteikolla A (Hyvä) - B (Toimiva) - C (Kehitettävä) - D (Riittämätön).

Yhteenvetona saatiin Tuusulan kunnan tietosuojan sisäisen valvonnan tilan olevan



Kuva 7 Sisäisessä tarkastuksessa esille nousseet tietosuojahavainnot

Tietosuoja oli yksi sisäisen tarkastuksen kohteista vuonna 2024. Sisäisessä tarkastuksessa arvioitiin Tuusulan kunnan tietosuojatyötä GDPR:n vaatimusten pohjalta.

toimivalla (B) -tasolla. Kuvassa 7 on kooste tehtyjen havaintojen määrästä ja riskin merkittävyydestä.

Eniten kehitettävää (havainnot tasolla C) tunnistettiin olevan tietosuojariskien dokumentoinnissa ja sovittujen toimenpiteiden seurannassa, tietosuojaselosteiden muodossa sekä rakennuslupiin liittyvien tietojen julkaisussa.

Tekniseen tietoturvaan tehtiin vuoden 2024 aikana useita parannuksia. Tärkeimpinä kokonaisuuksina kunnan tietoliikenneverkon ja Microsoft-ympäristön konfiguroinnit päivitettiin, monivaiheisen tunnistautumisen käyttöönottoa laajennettiin ja Microsoft-ympäristön lisenssitasoa nostettiin ennakoivan suojauksen parantamiseksi. Teknisillä muutoksilla on havaittu selkeä positiivinen vaikutus.

TIETOSUOJATYÖN TAVOITTEET 2025

Vuonna 2023 kirjattiin hallitusohjelmaan hallinnollisen seuraamusmaksun käyttöönotto tietosuojarikkomusten osalta myös julkisella sektorilla. Seuraamusmaksua ei otettu käyttöön vuoden 2024 aikana, sillä se vaatii isohkoja muutoksia nykyiseen lain-

säädäntöön. Tietosuojavaltuutetun toimisto edistää asiaa aktiivisesti ja on todennäköistä, että se tulee käyttöön seuraavan parin vuoden aikana. Henkilötietojen siirrot Euroopan ja Yhdysvaltojen välillä ovat helpottuneet komission tekemän riittävyyspäätöksen jälkeen, mutta tilanne on epävarma tulevaisuuden osalta. On syytä seurata tarkasti henkilötietojen siirtoihin liittyviä mahdollisia muutoksia.

EU:n tasolla on otettu käyttöön lainsäädäntöä, joka vaikuttaa kuntienkin toimintaan mm. tekoälyn käyttöä ja tiedonhallintaa koskien. Myös Tuusulan on syytä pysyä ajan tasalla EU:n muuttuvan regulaation osalta.

Tietosuojatyön osalta kehitämme toimintaamme seuraavasti vuonna 2025:

1. Tiedonhallintamallin dokumentointi Digiturvamalliin

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.

Digiturvamallin käyttöönotto aloitettiin vuonna 2024 ja sitä jatketaan edelleen vuonna 2025. Painopiste siirtyy nyt toimialueilla tehtävästä tiedonsyöttöön liittyvästä työstä sisällön ylläpitoon ja viimeistelyyn, joka tapahtuu kehittämisen ja tietohallinnon palvelualueen toimesta.

Digiturvamallin kautta saamme käyttöön mm. sisäisessä tarkastuksessa kehityskohteiksi mainitut suositusten mukaiset tietosuojaselosteet sekä henkilötietojen käsittelytoimien kuvauksen.

2. Riskienhallintaprosessin uudistaminen osana ka-ryhmän työtä

V. 2024 toimintansa aloitti kunnan kokonaisarkkitehtuuriryhmä, jonka tavoitteena on varmistaa erilaisten tietojärjestelmien yhteensopivuus, vaatimustenmukaisuus ja hallittu käyttöönotto. Arkkitehtuurihyväksyntäprosessin avulla pyritään yhdenmukaistamaan käytäntöjä tähän liittyen. Tietosuojariskit arvioidaan yhtenä osana arkkitehtuurihyväksyntäprosessia. Otetaan uusi toimintamalli tätä koskien käyttöön v. 2025.

3. Tietosuoja- ja tietoturvakoulutusalustan vaihtaminen

Toukokuussa 2025 vaihdamme tietosuoja- ja tietoturvakoulutusten järjestelmän ja siirrymme käyttämään Eduhouse-alustan tarjoamia koulutuksia. Eduhouse tarjoaa laajan koulutusvalikoiman julkishallinnon työntekijöille. Joukossa on runsaasti myös tietosuojaan ja tietoturvaan liittyviä koulutuksia, sekä mm. tekoälyn käyttöä koskevia koulutuksia. Pakolliset kurssit on valittu alustalta jo vuonna 2024 ja näitä alamme jalkauttaa työntekijöiden tietoon ja käyttöön toukokuussa.

4. Rakennuslupiin liittyvän tietosuojan tarkastelu ja kehittäminen

Sisäisessä tarkastuksessa erääksi kehityskohteeksi nousi rakennuslupiin liittyvä tietosuoja. Lainsäädäntö tätä koskien on monimutkainen ja vaikeaselkoinen. Käydään rakennuslupiin liittyvät käytännöt läpi tietosuojan osalta ja laaditaan ohjeet yhdessä toimialueen kanssa.

5. Teknisen tietoturvan parantaminen

Tarkastelemme Microsoft-ympäristömme tietoturvaa ja kehitämme sitä edelleen osana jatkuvuudenhallintatyötämme. Tukeudumme teknisesti entistä vahvemmin kunnan yhteisiin alustaratkaisuihin, joihin kuuluvat mm. sähköisen asioinnin ja tiedolla johtamisen sekä käyttövaltuushallinnan alustat. Vakioimme arkkitehtuurihyväksynnän prosessin ja laajennamme monivaiheisen tunnistautumisen koko organisaation kattavaksi.

Vuoden 2025 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.