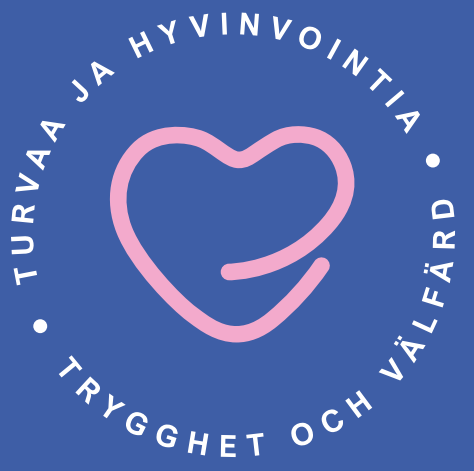


Tietosuojavastaavan katsaus vuoteen 2023

Tietosuojavastaava Sebastian Ekblom

Itä UUSIMAA
Östra NYLAND
Hyvinvointialue
Välfärdsområde

Tiivistelmä

Tämän raportin tarkoituksena on lyhyesti katselmoida Itä-Uudenmaan hyvinvointialueen vuoden 2023 toimintaa tietosuojan ja tietosuojavastaavan näkökulmasta. Itä-Uudenmaan hyvinvointialueen ensimmäinen vuosi piti sisällään paljon kehittämistä eri osa-alueilla, näin myös tietosuojan osalta. On haastavaa saada vuodessa kaikki prosessit ja ohjeet jalkautettua siten, että toimintatavat olisivat kaikille selviä. Kaikilla lähtöorganisaatioilla oli erilaisia toimintatapoja, ja niiden yhtenäistäminen tulee viemään jonkin aikaa.

Tietosuoja ja siihen liittyvä työ ja dokumentointi on kuitenkin organisaatiosta riippumatta hoidettava tietosuoja-asetuksen (GDPR) mukaisesti. Vuoden aikana perustettiin tietosuojatyöryhmä, jonka päätehtävä on valvoa ja keskustella ajankohtaisista aiheista tietosuojan näkökulmasta, sekä tehdä tarvittavia linjauksia, jos huomataan että johonkin tarvitaan tarkempaa linjausta tai ohjeistusta. Tietosuojatyöryhmä koostuu eri yksiköiden työntekijöistä ja esihenkilöistä läpi koko organisaation, jotta parhaiten saadaan tietoja eri yksiköistä ja niiden senhetkisistä tilanteista. Tietosuojatyön avuksi hankittiin tietosuojavastaavan valmistelun pohjalta Agendium Oy:n tarjoama Digiturvamalli - tietosuojatyökalu, joka otettiin käyttöön loppusyksystä 2023.

Koska kyseessä on Itä-Uudenmaan hyvinvointialueen ensimmäisen toimintavuoden raportointi, vielä ei pystytä tekemään niin yksityiskohtaisia päätelmiä tietosuojan osalta. Siitä syystä raportissa ei myöskään ole vertailutietoa aikaisempiin vuosiin eikä mennä kovin yksityiskohtaisiin lukuihin. Vuoden 2024 kohdalla tilanne tulee olemaan toinen ja seuranta jatkossa pystytään tekemään paremmin myös reaaliajassa.

Sisällys

1 Tietosuojan toteuttaminen

Itä-Uudenmaan hyvinvointialueen toiminnan alussa vuonna 2023 hallintolakimies hoiti tietosuojavastaavan tehtäviä. Tietosuojatyön ja sen implementointi hyvinvointialueen kokoisessa organisaatiossa on kuitenkin laaja osa-alue ja toimintojen yhtenäistäminen myös tietosuojatyön osalta vaatii resursseja ja vie aikaa. Tietosuojatyö ei ole projektiluonteista, vaan se vaatii ennakointia, jatkuvaa seurantaa ja sitä, että puutteisiin puututaan mahdollisimman nopeasti silloin kun niitä havaitaan.

Huhtikuussa 2023 tietosuojavastaavan tehtävään valittiin Sebastian Ekblom, joka aikaisemmin toimi Porvoon kaupungin sosiaali- ja terveystoimen johdossa sovellusasiantuntijana, sekä myöhemmin järjestelmäasiantuntijana Itä-Uudenmaan hyvinvointialueella.

Tietosuojavastaavan tehtävänkuva on kansallisten määritysten mukainen ja sisältää paljon yhteistyötä myös Tietosuojavaltuutetun toimiston kanssa. Tietosuojavaltuutetun toimisto toimii valtion Oikeusministeriön alaisuudessa. Tietosuojavastaavan tehtävä sijoittuu hallintopalveluihin hallintojohtajan alaisuuteen, vaikkakin tietosuojavastaavan toimi on riippumaton. Tietosuojavastaavan kannanottoihin ei saa yrittää vaikuttaa. Tietosuojavastaavalla on myös oikeus saada perustelut, jos päätetään toimia toisin kuin tietosuojavastaava on suositellut.

Tietosuojavastaava työskentelee suurimmaksi osaksi itsenäisesti tai yhteistyössä hyvinvointialueen lakimiestiimin kanssa. Tietosuojavastaavan toiveena on, että henkilöstö on matalalla kynnyksellä yhteydessä, jos joku asia mietityttää tietosuojaan liittyen tai jos on tapahtunut esim. tietosuojaloukkaus. Tietosuojavasta keskustelee jatkuvasti myös johdon kanssa, jotta tiedonkulku on jatkuvaa ja molemminpuolista.

1.1 Tietosuojaan liittyvä lainsäädäntö

Tietosuojaan ja siihen liittyvä työ perustuvat EU:n tietosuoja-asetukseen (GDPR 679/2016) ja Tietosuojalakiin (1050/2018). Vuoden 2024 alusta voimaan tullut Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) ohjaa myös tietosuojaan liittyviä asioita ja henkilötietojen käsittelyä. Laki viranomaisen toiminnan julkisuudesta (621/1999) on myös keskeinen laki tietosuojavastaavan työssä. Näiden lisäksi löytyy muuta lainsäädäntöä ja erilaisia asetuksia.

1.2 Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtävistä säädetään EU:n tietosuoja-asetuksessa (GDPR 679/2016 39 artikla).

1. Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät:

> a. antaa rekisteri- tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden tämän asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia;

b. seurata, että noudatetaan tätä asetusta, muita unionin tai jäsenvaltion tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset;

c. antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti;

d. tehdä yhteistyötä valvontaviranomaisen kanssa;

e. toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

2. Tietosuojavastaavan on tehtäviään suorittaessaan otettava asianmukaisesti huomioon käsittelytoimiin liittyvä riski ottaen samalla huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

1.3 Tietosuojavastaavan asema

Tietosuojavastaava on tehtävässään riippumaton eikä hän saa ottaa vastaan ohjeita asetuksen mukaisten tehtävien hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Tehtäviään suorittaessa tietosuojavastaavaa sitoo salassapitovelvollisuus Euroopan unionin lainsäädännön tai kansallisen lainsäädännön mukaisesti.

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana. Muilta osin häntä koskee sama sopimus- tai palvelusuhdelainsäädäntö. Huomioitavaa on myös, että tietosuojavastaavana ei voi toimia henkilö, joka samaan aikaan työtehtäviensä kautta määrittää tietojenkäsittelyn tarkoitukset ja keinot.

1.4 Tietosuojavastaavan vastuut

Tietosuojavastaava ei ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen noudattamatta jättämisestä, jos asetusta ei ole noudatettu. Tietosuojasäännösten noudattaminen on aina rekisterinpitäjän ja/tai henkilötietojen käsittelijän vastuulla.

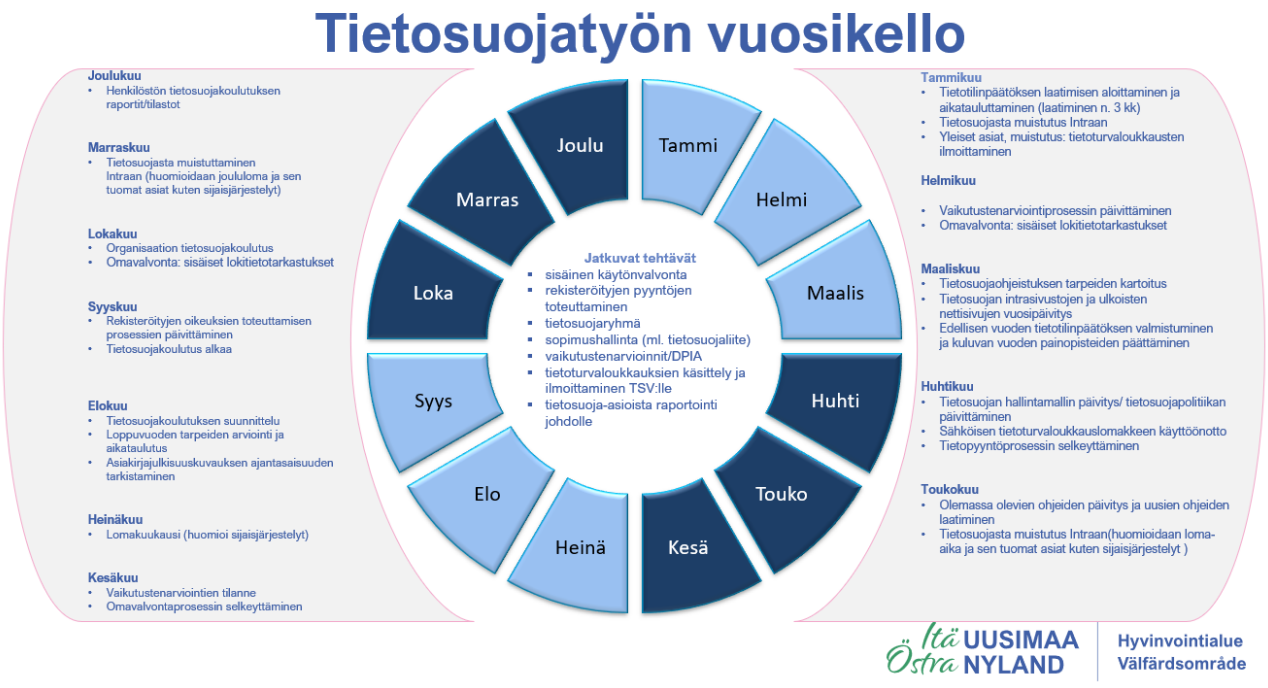
Jos rekisterinpitäjä tai henkilötietojen käsittelijä tekee päätöksiä, jotka eivät ole yleisen tietosuoja-asetuksen ja tietosuojavastaavan neuvojen mukaisia, suositeltavaa olisi antaa tietosuojavastaavalle tilaisuus esittää eriävä mielipiteensä ylimmälle johdolle ja päätöksentekijöille. Mahdollisissa erimielisyystilanteissa on suositeltavaa dokumentoida perusteet, joiden vuoksi tietosuojavastaavan neuvoa ei noudateta.

1.5 Tietosuojatyöryhmä tietosuojavastaavan tukena

Itä-Uudenmaan hyvinvointialuejohtajan kesällä 2023 tekemällä päätöksellä perustettiin tietosuojatyöryhmä. Tietosuojaryhmään kuuluu työntekijöitä eri yksiköistä ja eri asemista. Tietosuojatyöryhmä kokoonpano oli seuraava, toiminnan lähtiessä käyntiin viime kesänä:

- hoitotyön johtaja
- johtava lakimies (sihteeri)
- johtava lääkäri
- pelastustoimen edustaja
- sosiaalityön johtaja
- tietosuojavastaava (puheenjohtaja)
- tietoturvapäällikkö
- tietohallintopäällikkö (varapuheenjohtaja)

Näiden ohella ryhmään kutsutaan tarpeen mukaan myös muita asiantuntijoita, jos käsittelyssä on joku erityinen aihe. Tietosuojavastaava toimii ryhmän puheenjohtajana, ja jokainen edustaja saa vapaasti tuoda omia asioita/kysymyksiä kokouksiin. Vuoden 2023 aikana ryhmä kokoontui syksyn aikana viisi kertaa. Tietosuojatyön suunnittelussa on käytössä myös tietosuojatyön vuosikello.



2 Itä-Uudenmaan hyvinvointialueen tietovarannot

Tietovarannolla tarkoitetaan tietojen muodostama tietoaineisto tai kokoelma tiettyä tarkoitusta varten. Tietovarannot Itä-Uudenmaan hyvinvointialueella koostuu alla olevista kokonaisuuksista: sosiaalihuollon, terveyshuollon sekä pelastustoimen palveluja tukevat tietovarannot. Näiden lisäksi konserni- ja strategiapalvelulla on omat tietovarantonsa.

Hyvinvointialueen verkkosivuilla julkaistavan asiakirjajulkisuuskuvauksen tarkoituksena on auttaa asukkaita hahmottamaan paremmin mihin heidän tietojansa tallennetaan sekä miten niitä käsitellään Itä-Uudenmaan hyvinvointialueella.

Sosiaali- ja terveyspalveluiden tarjoamiseksi tietoja luovutetaan lakisääteisesti. Tietojen luovutuskohteita voivat olla Kansaneläkelaitos (Kela), muut tiedonsaantiin oikeutetut viranomaiset ja vakuutusyhtiöt.

Yhteistyökumppaneita, joiden kanssa tiedonvaihto perustuu lakisääteisiin tietojenluovutuksiin, ovat esimerkiksi palveluseteli- ja ostopalvelua tarjoavat yhteistyöyritykset ja lääketutkimusyhteistyökumppanit.

2.1 Asiakastiedot

Asiakastiedot sisältävät Itä-Uudenmaan hyvinvointialueen sosiaalipalveluiden asiakkaiden tiedot sekä asiakirjat. Nämä ovat salassa pidettäviä.

Tietoaineistot:

- Asiakashallinnolliset tiedot
- Asiakasrekisterit

2.2 Potilastiedot

Potilastiedot sisältävät Itä-Uudenmaan hyvinvointialueen terveyspalveluiden asiakkaiden henkilötiedot sekä potilasasiakirjat. Nämä ovat salassa pidettäviä. Potilasasiakirjat ovat potilaan hoidon järjestämisessä ja toteuttamisessa käytettäviä, terveydenhuollossa laadittuja asiakirjoja. Nämä voivat myös koostua saapuneista asiakirjoista tai tallenteista.

Tietoaineistot:

- Potilashallinnolliset tiedot
- Potilasrekisteri
- Potilaan ajanvaraustiedot

2.3 Pelastustoimen tiedot

Pelastustoimelle määrätyt tehtävien järjestämiseen tarvittavat tiedot tallennetaan pelastustoimen tietovarantoon. Pelastustoimen tiedoissa on sekä julkisia että salassa pidettäviä tietoja. Vuoden 2024 alusta Laki hätäkeskustoiminnan annetun lain muuttamisesta 438/2023 astui voimaan siltä osin, että hyvinvointialueet tulevat jatkossa toimimaan rekisterinpitäjinä hätäkeskuksessa käsiteltäviin tietoihin.

Tietoaineistot:

- Pelastustoimintaan osallistuvien henkilörekisteri
- Valvontarekisteri
- Toimenpiderekisteri
- Varautumisen tietovaranto

2.4 Konserni- ja strategiapalvelut

Itä-Uudenmaan hyvinvointialueen konserni- ja strategiapalveluiden tietovaranto sisältää hyvinvointialueen johtamiseen ja päätöksentekoon, kehittämiseen, ohjaamiseen, seurannan ja valvonnan sekä yhteisten tukipalveluiden muodostamat tietokokonaisuudet.

Tietoaineistot:

- Asianhallintarekisteri
- Sopimusrekisteri
- Luottamushenkilörekisteri
- Sidosryhmätiedot
- Viestintä
- Henkilöstö
- Talous
- Tilastointi
- Palautteet
- Tietoturvaloukkausilmoitukset
- Haitta- ja vaaratapahtumailmoitukset

3 Rekisteröidyn oikeuksien toteutuminen

Rekisteröidyn oikeuksien toteutuminen sosiaali- ja terveyshuollossa sekä pelastustoimessa on tärkeä osa henkilötietojen suojaa ja yksilön oikeuksien kunnioittamista. Euroopan unionin yleinen tietosuoja-asetus (GDPR) sekä kansalliset lait tarjoavat rekisteröidyille henkilöille tietyt oikeudet, joiden avulla he voivat hallinnoida henkilötietojaan. Nämä oikeudet ovat erityisen merkittäviä sosiaali- ja terveyshuollon sekä pelastustoimen osalta, joissa käsitellään paljon arkaluonteisia henkilötietoja. Alla on avattu tarkemmin, miten oikeudet toteutuvat kyseisillä aloilla:

1. Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada pääsy itseään koskeviin henkilötietoihin. Sosiaali- ja terveyshuollossa tämä tarkoittaa esimerkiksi potilaskertomusten ja hoitosuunnitelmien saatavuutta. Pelastustoimessa tämä voi tarkoittaa tietoja, jotka liittyvät henkilön osallistumiseen pelastustoimen toimintaan tai onnettomuustietoja.

2. Oikeus tietojen oikaisemiseen

Mikäli rekisteröity huomaa, että häntä koskevat tiedot ovat virheellisiä tai puutteellisia, hänellä on oikeus pyytää näiden tietojen oikaisemista. Tämä on erityisen tärkeää, sillä virheelliset tiedot voivat vaikuttaa henkilön saamaan hoitoon tai palveluihin. Jos johtava lääkäri kokee, että tietojen oikaisemista ei voida toteuttaa rekisteröidyn pyynnön mukaisesti, siitä tehdään kielteinen päätös, johon liitetään oikaisuvaatimusohje.

3. Oikeus tietojen poistamiseen

Tietyissä olosuhteissa rekisteröidyllä on oikeus pyytää henkilötietojensa poistamista. Sosiaali- ja terveyshuollossa tämä oikeus voi olla rajoitettu, koska lainsäädäntö velvoittaa säilyttämään potilasasiakirjoja määritellyn ajan. Tässäkin pätee sama kuin kohdassa 2: jos johtava lääkäri arvioi, että tietojen poistamiseen ei ole perusteita rekisteröidyn pyynnön mukaisesti, siitä tehdään kielteinen päätös, johon liitetään oikaisuvaatimusohjeistus. Tietojen poistaminen sosiaali- ja terveystoimessa sekä pelastustoimessa on harvinaista.

4. Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus pyytää henkilötietojensa käsittelyn rajoittamista tietyissä tilanteissa. Esimerkiksi, jos henkilö kiistää tietojen paikkansapitävyyden, hän voi pyytää käsittelyn rajoittamista, kunnes tiedot on tarkistettu.

5. Oikeus tietojen siirrettävyyteen

Tämä oikeus mahdollistaa henkilötietojen siirtämisen yhdestä järjestelmästä toiseen sähköisessä muodossa. Sosiaali- ja terveyshuollossa tämä voi helpottaa potilaan tietojen siirtämistä eri palveluntarjoajien välillä.

6. Oikeus vastustaa käsittelyä

Rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä tietyissä tilanteissa, kuten suoramarkkinoinnissa. Sosiaali- ja terveyshuollossa sekä pelastustoimessa tämä voi koskea esimerkiksi tietojen käyttöä tutkimustarkoituksiin.

7. Oikeus tehdä valitus valvontaviranomaiselle

Jos rekisteröity katsoo, että hänen tietosuojaoikeuksiaan on loukattu, hänellä on oikeus tehdä valitus kansalliselle tietosuojaviranomaiselle, Tietosuojavaltuutetun toimistolle.

Näiden oikeuksien toteutuminen edellyttää organisaatioilta selkeitä prosesseja ja käytäntöjä henkilötietojen käsittelyssä. Sosiaali- ja terveydenhuollon sekä pelastustoimen osalta on varmistettava, että henkilöstö on koulutettu ja että oikeudelliset ja eettiset velvoitteet henkilötietojen käsittelyssä tunnistetaan ja niitä noudatetaan. Tässä korostuu johtavien viranhaltijoiden osaaminen, sillä rekisterin omistaja viime kädessä päättää tietojen luovutuksesta. Tällaisissa tapauksissa myös tietosuojavastaava usein toimii apuna ja antaa neuvoja.

3.1 Rekisteri- ja lokitietojen tarkastuspyynnöt

Vuoden 2023 aikana Itä-Uudenmaan hyvinvointialueelle tuli 303 kpl asiakkaiden tekemiä tarkastuspyyntöjä koko hyvinvointialueen osalta. Tämä luku sisältää sekä rekisteritietojen tarkastuspyynnöt että lokitietojen tarkastuspyynnöt.

Sosiaalihuoltoon liittyviä tarkastuspyyntöjä tuli 145 kpl ja terveydenhuoltoon liittyviä 164 kpl. Rekisteritietojen korjauspyyntöjä tuli vuoden aikana 6 kpl ja kaikki olivat terveydenhuoltoon liittyviä; sosiaalihuoltoon korjauspyyntöjä ei tullut yhtään vuoden 2023 aikana.

Pelastuslaitoksen osalta pyyntöjen tarkka seuraaminen on ollut haastavampaa, sillä rekisterinpitäjä on ollut Hätäkeskuslaitos, eikä pyyntöjä siten ole ollut mahdollista tilastoida hyvinvointialueen kirjaamossa. Tämä tulee kuitenkin jatkossa olemaan helpompaa, kun Hätäkeskuslaki muuttui vuoden 2024 alussa, ja näin ollen hyvinvointialueista tulee rekisterinpitäjiä myös hätäkeskustoimintojen tietojen osalta. Jatkossa tarkastuspyynnöt näiden tietojen osalta osoitetaan myös hyvinvointialueille.

4 Henkilöstön tietosuojaosaaminen

Henkilöstön tietosuojaosaamisen osalta on eroja eri yksiköiden välillä. Myös yksiköiden ja eri ammattiryhmien sisällä on vaihtelua.

Tietosuoja arjessa ei ole vielä jokapäiväistä kaikille, eikä näin ollen luonnistu yhtä hyvin kaikilta. Tietosuojaosaamisen parantamiseksi koko henkilöstön tasolla otettiin viime vuonna käyttöön Navicren tarjoama Navisec -tietosuoja ja tietoturvakoulutusohjelma.

Johto on yhdessä tietosuojavastaavan kanssa linjannut, että koulutus on suoritettava hyväksytyksi joka vuosi tai työsuhteen alkaessa. Vuonna 2023 koulutus suoritettiin lokakuusta joulukuun loppuun mennessä. Koulutus koostuu neljästä pääosiosta: henkilötietojen käsittely, GDPR organisaatiossa, tietosuoja sosiaalihuollossa ja tietosuoja terveydenhuollossa. Kaikkia pyydettiin suorittamaan kaikki neljä osaa, paitsi ruoka- ja kiinteistöhuoltoon kuuluvat, joita pyydettiin suorittamaan kaksi ensimmäistä osaa.

Vuoden 2023 loppuun mennessä koulutuksen suoritustilanne per koulutuskokonaisuus:

(Tilastot otettu 24.1.2024)

Henkilöstön tietoturva ja tietosuoja	1928 henkilöä
Henkilötietoja käsittelevien GDPR-koulutus	1700 henkilöä
Terveydenhuollon tietoturva ja tietosuoja	1612 henkilöä
Sosiaalihuollon tietoturva ja tietosuoja	1621 henkilöä

Pelastustoimen henkilöstö suoritti Graniten tarjoaman vastaavan tietosuoja- ja tietoturvakoulutuksen, joka tämän vuoden osalta vastasi hyvinvointialueen Navisec -koulutusta. Jatkossa olisi toivottavaa, että koko organisaatio tekisi saman koulutuksen. Silloin myös vertailu ja seuranta henkilöstöryhmien kesken olisi helpompaa.

4.1 Tietosuoja- ja tietoturvaloukkaukset

Itä-Uudenmaan hyvinvointialueen tietosuojavastaavan on ilmoitettava Tietosuojavaltuutetun toimistolle, jos saa tietoonsa tietosuojaloukkauksen, jossa epäillään henkilötietojen joutuneen vääriin käsiin. Ilmoitus on tehtävä viipymättä, kuitenkin korkeintaan 72 h sisällä siitä, kun tietosuojaloukkaus tulee ilmi.

Vuoden 2023 aikana Itä-Uudenmaan hyvinvointialueen tietosuojavastaava teki yhteensä 23 tietoturvaloukkausilmoitusta Tietosuojavaltuutetun toimistolle, heidän sivuillaan olevan sähköisen lomakkeen kautta. Näistä kaikista, kaksi oli luonteeltaan vakavia ja niistä tehtiin myös tutkintapyyntö poliisille.

Yleisesti voi todeta, että suurin osa tietosuojaloukkauksista johtui työntekijöiden huolimattomuudesta kiireen keskellä. Sähköpostiviesti, joka vahingossa lähti väärälle vastaanottajalle, oli usein esille noussut ongelma. Joissakin tapauksissa oli liitteitä mukana, jotka sisälsivät salassa pidettävää tietoa. Myös tekstiviestimuistutukset menivät useamman kerran väärälle potilaalle, koska potilastietoihin oli tallennettu väärä puhelinnumero.

5 Arviointi ja kehittäminen

5.1 Arviointi

Kun katsoo koko organisaatiota, hyvinvointialueella on hyvä pohja ja tietojen käsittelyä turvataan erilaisilla suojaustoiminnoilla. Mitä tulee dokumentointiin, löytyy parannettava. Kuten aikaisemmin todettiin, vuoden aikana ei tämän kokoista kokonaisuutta saada valmiiksi siten, että se olisi riittävän selkeä kaikille.

Tietosuojaa koskeva vaikutusten arviointi (DPIA:ksi – Data Protection Impact Assessment) ja niiden tekeminen hankintojen yhteydessä, tulee aina tehdä, jos on tarkoitus käsitellä henkilötietoja. DPIA:n tekemiseen on tullut enemmän rutiinia ja koko ajan yritetään muistuttaa siitä, että sellainen on oltava ennen kuin hankinta voidaan hyväksyä. Tämä osa parantui sisäisen ICT-hankintaryhmän perustamisen myötä, ja siellä käydään läpi ajankohtaiset hankintapyynnöt, jotka ovat tulleet kentältä.

Osa järjestelmien tai sovellusten vaikutusten arvioinneista puuttuu. Niiden tekeminen on aikaa vievää ja vaatii suunnittelua. Tietosuojavastaavan resurssit kuitenkin ovat rajalliset. Päävastuu vaikutusten arvioinnissa on hankinnan omistajalla. Tietosuojavastaava on mukana auttamassa ja ohjeistamassa sen tekemisessä, vetovastuu kuitenkin on hankinnan omistajalla.

Ohjeistuksiin ja erinäisiin linjanvetoihin on myös yritetty panostaa, näistä keskustellaan usein tietosuojaryhmän kokouksissa. Mallipohjia erilaisiin päätösteksteihin ja ohje alaikäisen päätöksentekokyvyn arvioimiseksi on työn alla.

Tietosuojatyöryhmä kokoontui viisi kertaa syksyllä 2023.

5.2 Kehittäminen

Koulutustarvetta on ympäristön jatkuvasti kehittyessä. Tämä tuo tullessaan uusia mahdollisuuksia, mutta niissä piileskelee myös aina tietosuojaan liittyvä uhka, joka on tärkeää huomioida ja siihen kannattaa suhtautua vakavasti.

Seuraavana ilmiönä on jo vahvaa tuloa tekevä tekoäly (AI – Artificial Intelligence). AI tuo paljon mahdollisuuksia, jos sitä käytetään oikein, muussa tapauksessa se voi aiheuttaa koko organisaatiolle erilaisia haasteita. Tärkein asia tässä on saada henkilöstö ymmärtämään, että AI-järjestelmiin ei kannata antaa mitään tunnistetietoja, joita AI voi hyödyntää, ja että ne tallentuvat jatkokäyttöä varten. Toki on myös muistettava, että kaikki tiedot, jotka sieltä

saadaan, ei välttämättä ole täysin validia, eli käyttäjän on oltava kriittinen ja myös tarkistaa paikkansapitävyyden.

Vaikka tietosuojavastaavan kuuluu valvoa tietosuojaa ja henkilötietoja käsittelyä, tekoälyyn tulee kuitenkin suhtautua myönteisesti, koska tekoälyä voi joissakin osa-alueilla hyödyntää monessa ja tehostaa työtä ja säästää aika.

6 Seuranta

Tietosuojatyö ei ole projektiluonteista, eikä sitä myöskään koskaan saada kirjaimellisesti valmiiksi. Tietosuojaa kehitetään sen mukaan, miten organisaatio kehittyy, uudet järjestelmät vaativat vaikutusten arvioinnin tekoa, uudet työntekijät pitää kouluttaa, rekisteriselosteet on koko ajan pidettävä ajan tasalla. Tämä on kuitenkin vain pieni osa jatkuvaa työtä, joka koostuu monesta eri osasta.

Jatkossa on kuitenkin helpompaa seurata ja vertailla kun käytössä on vuoden 2023 luvut pohjana (tietoturvaloukkausten määrät ja miten niiden kehitys etenee). Tavoitteena toki on, että tietosuojatyön kautta saadaan myös sisäisesti tietosuojaloukkausten määrät vähenemään. On tärkeää, että myös esihenkilötasolla jatkuvasti muistutetaan työntekijöitä tietosuojan tärkeydestä. Kaikki pystyvät vaikuttamaan siihen. Seuranta ja valvonta tapahtuu myös sisäisesti lokitietojen tarkastuksilla.

6.1 Lokitietojen tarkastukset osana omavalvontaa

Lokitietojen tarkastus henkilöstön osalta suoritetaan noin 2–3 kertaa vuodessa. Jos on tarvetta, suoritetaan ylimääräisiä tarkistuksia. Säännöllisessä lokitietojen tarkastuksessa sisäinen tarkastaja valitsee satunnaisotoksella noin kaksi henkilöä per asiakas- ja potilastietojärjestelmä. Jotkut järjestelmät ovat jaettu eri osiin riippuen mistä kokonaisuudesta koostuu, siksi eivät tarkkaan täsmää järjestelmien määrien kanssa. Lokitietojen tarkastus on tärkeä osa organisaation omavalvontaa. Lokitarkastuksen toteuttaminen on haastavampaa nyt kun organisaatiossa vielä on monta erilaista hyvinvointialueelle siirtynyttä kuntien entistä asiakas- ja potilastietojärjestelmää.

Lokitarkastukset aloitettiin syksyllä 2023 jolloin pyydettiin noin 22 henkilöstöön kuuluvan lokitietoja syyskuun ajalta. Heistä 8 työntekijän osalta löydettiin lokitietoja tarkastettavaksi. Tarkastuksessa pyydettiin kokonaan noin 22 työntekijän lokitiedot. Tämä osittain antaa ymmärtää, että tunnuksia järjestelmiin on ollut, vaikkei niihin ole ollut aktiivista käyttöä.

6.2 Tämänhetkinen tilanne ja ideoita jatkoa ajatellen

Tällä hetkellä työn alla olevia asioita ja pari ideaa jatkokehitykseen:

- Tarkastuspyyntö -lomakkeet asukkaille kehitetään, jotta jatkossa olisivat selkeämpiä
- Työn alla on lomake hyvinvointialueen työntekijöille, jonka kautta voi ilmoittaa tietosuojaloukkauksesta
- Digiturvamallin käytön tehostaminen/dokumentoinnin parantaminen
- Turvapostin käytön tehostaminen – paperien vähentäminen
- Suomi.fi -viestit käyttöönotto - viranomaisposti

7 Päätössanat

Itä-Uudenmaan hyvinvointialueen ensimmäinen vuosi tietosuojan ja tietosuojavastaavan näkökulmasta sujui suhteellisen hyvin, siihen nähden miten paljon työtä ja kehittämistä on ollut. Erilaisia toimintatapoja ja käytäntöjä aikaisemmista organisaatioista on aikaa vievää yhtenäistää. Aina löytyy myös parannettavaa ja kehitettävää.

Digiturvamalli, tietosuojatyökalu, joka otettiin käyttöön viime kesänä, tulee olemaan tärkeä työkalu toiminnan kehittämisessä tietosuojatyön kannalta. Sovelluksen avulla on helpompaa arvioida riskit ja uhat, ja myös täyttää osoitusvelvollisuuden ja tietosuoja-asetuksen (GDPR) muut asettamat vaatimukset.

Lopuksi pienet teot, joilla on erittäin suuri vaikutus. Toivottavasti se olisi kaikille itsestäänselvyys – kun jätät tietokoneesi vartioimatta, muista aina lukita se. Jos kyseessä on paperilla olevia tietoja, laita ne lukittuun kaappiin/laatikkoon.