TIETOTILINPÄÄTÖS 2024
Satakunnan hyvinvointialue

25.2.2025 aluehallitus

TIETOTILINPÄÄTÖS 2024

1. JOHDANTO
   - Tietotilinpäätös
2. TIEDONHALLINTA
   - Tietovarannot
3. LAINSÄÄDÄNTÖ JA MUU OHJEISTUS
   - Tietosuojaperiaatteet
   - Tietojen käsittelyn periaatteet
4. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN
   - Tietosuojan ja tietoturvallisuuden hallintamalli
   - Tietosuojavastaava
   - Tietosuojan vaikutustenarvioinnit
   - Lokivalvonta
   - Sopimukset ja hankinnat
   - Koulutukset ja ohjeistus
   - Tietoturva ja jatkuvuudenhallinta
   - Tieteellinen tutkimus
5. REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN
   - Rekisteröidyn oikeudet
   - Tietopyynnöt
   - Tietoturvaloukkaukset
   - Valvontaviraomasten selvitys- ja tietopyynnöt
6. ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN
   - Tietosuojatyössä havaitut ongelmakohdat, kehittämistarpeet ja onnistumiset

1. JOHDANTO

EU:n tietosuoja-asetus ja kansallinen tiedonhallintalaki ovat tuoneet merkittävästi uusia vaatimuksia sekä tiedonhallintaan että tietojärjestelmiin ja prosesseihin.

Rekisterinpitäjä on vastuussa siitä, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia.

Tietotilinpäätös ei ole asetuksen vaatimus, mutta se on suositeltava tapa vastata tietosuoja-asetuksen osoitusvelvollisuuteen ja raportoida johdolle.

Tietotilinpäätös on osa tietojohtamista, sekä siihen kuuluvaa riskienhallintaa ja sisäistä valvontaa.

Psykoterapiakeskus Vastaamoon kohdistunut tietomurto on tuonut kaikkien tietoisuuteen sen, mihin puutteet tietosuojassa ja tietoturvassa voivat pahimmillaan johtaa.

Ukrainan sodasta johtuva kriisialtis maailmantilanne lisäsi merkittävästi tietosuojan ja tietoturvan merkitystä riskienhallinnassa.

1.1 Tietotilinpäätös

- antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
- kuvaa mitä tietovarantoja organisaation hallussa on
- kuvaa organisaation toimintaan liittyvät tietovirrat
- kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
- kuvaa miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
- kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
- toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
- toimii raportoinnin ja johtamisen tukena organisaatiossa
- toimii kehittämistoimenpiteiden seurannan apuvälineenä
- toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
- varmistaa sovellettavan lainsäädännön noudattamisen

2. TIEDONHALLINTA

Laissa julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki 906/2019) säädetään julkisuusperiaatteen ja hyvän hallinnon periaatteista viranomaisten tiedonhallinnassa. Laissa säädetään myös tietojärjestelmien yhteentoimivuudesta ja tietoturvallisuuden toteuttamisesta.

Tiedonhallintalain edellyttämän tiedonhallintamallin laatiminen parantaa kokonaisarkkitehtuurityön kypsyystasoa, kun organisaation prosessit, tietovarannot, tietoaineistot ja järjestelmät on kuvattu yhtenäiseksi kokonaisuudeksi ja niistä saadaan kattava näkymä kehittämisen ja hankintojen tueksi.

Satakunnan hyvinvointialueen keskeiset tietovarannot ja tietojärjestelmät on kuvattu tiedonhallintamallissa, jota ylläpidetään ARC-ohjelmistolla.

- Tiedonhallintamalli sisältää tietojärjestelmärekisterin, johon kuvataan tietojärjestelmien käyttötarkoitus, kriittisyys, elinkaari ja muut olennaiset tiedot tietojärjestelmistä. Henkilötietovarannoille on merkitty käyttötarkoitukset ja niihin sisältyville tietoaineistoille on määritelty säilytysajat.

Tiedon elinkaarta hallitaan tiedonohjaussuunnitelman avulla, johon on määritelty asiakirjojen säilytysajat, säilytysmuodot, julkisuus sekä muut tarvittavat metatiedot. Tiedonohjaussuunnitelmaa ylläpidetään tiedonohjausjärjestelmässä, johon määritellään myös tietojärjestelmien ulkopuolella olevan tiedon säilytysajat. Tiedonohjaussuunnitelma sisältää siten arkistonmuodostussuunnitelmalta edellytettävät tiedot.

Tiedonhallintalain edellyttämä asiakirjajulkisuuskuvaus on julkaistu hyvinvointialueen nettisivuilla.

Ulkopuolisia henkilötietojen käsittelijöitä ovat muun muassa in house -yhtiöt, ostopalvelujen tuottajat ja tietojärjestelmien palveluntuottajat. Ulkopuolisten henkilötietojen käsittelijöiden tuottama tieto sisältyy hyvinvointialueen tietovarantoihin.

2.1 Tiedonhallinnan käsitteitä

Tietovarannot

- Loogiset tietovarannot tarkoittavat viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettävää tietoaineistoja sisältävää kokonaisuutta, jota käsitellään tietojärjestelmien avulla tai manuaalisesti

Henkilötietovarannot

- henkilörekisterien pohjalta muodostettuja kokonaisuuksia, joissa käsitellään henkilötietoja.

Tietoaineistot

- asiakirjoista ja muista vastaavista tiedoista muodostuvia tiettyyn viranomaisen tehtävään tai palveluun liittyviä tietokokonaisuuksia, jotka tulevat suoraan tiedonohjaussuunnitelmasta.

Selosteet käsittelytoimista (GDPR)

- Rekisterinpitäjän on ylläpidettävä tietosuoja-asetuksen 30 artiklan mukaisia selosteita käsittelytoimista. Selosteet ovat yleisiä kuvauksia siitä, miten rekisterinpitäjä käsittelee henkilötietoja.
- Laaditaan organisaation sisäiseen käyttöön sekä valvontaviranomaisia varten.
- Ylläpidetään ARC-järjestelmässä, tiedonhallintamallin yhteydessä

3. LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Tietojen käsittely ja tietosuojaan liittyvä työ perustuvat EU:n tietosuoja-asetukseen (GDPR 679/2016) ja tietosuojalakiin (1050/2018), Lakiin julkisen hallinnan tiedonhallinnasta (tiedonhallintalaki 906/2019) ja lakiin viranomaisen toiminnan julkisuudesta (julkisuuslaki 621/1999) sekä asiakastietojen osalta Lakiin sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) sekä useisiin toimialaan liittyviin erityislakeihin.

Lisäksi organisaatiolla tulee olla omia ohjeita ja käytänteitä, jotka ohjaavat tietojen käsittelyä, mm:

- tietosuoja- ja tietoturvapolitiikka
- tietoturvasuunnitelma
- tietosuojan ja tietoturvallisuuden hallintamalli
- ohjeet asiakastietojen käsittelystä ja kirjaamisesta
- ohjeet asiakastietojen käytön valvonnasta (lokivalvonta)

3.1 Tietosuojaperiaatteet

Kaikki henkilötietoihin kohdistuvat toimenpiteet suunnittelusta keräämiseen, käsittelyyn ja henkilötietojen poistamiseen ovat henkilötietojen käsittelyä. Tietosuojaperiaatteita on noudatettava koko henkilötietojen käsittelyn elinkaaren ajan.

Tietosuojaperiaatteiden mukaan henkilötietoja on

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

3.2 Tietojen käsittelyn periaatteet

EU:n tietosuoja-asetuksen mukaisista käsittelyperusteista säädetään 6 artiklassa ja sitä täydentävässä tietosuojalain 4 §:ssä, sekä erityisiin henkilötietoryhmiin kuuluvien tietojen osalta 9 artiklassa ja tietosuojalain 6 §:ssä.

- Asiakastietoja käsitellään ja kirjataan asiakastietolain (703/2023) ja STM:n oppaan (STM 12/2024) mukaisesti.
- Ammattilaisille luodaan työtehtävän mukaiset käyttöoikeudet tietojärjestelmiin. Tietoja saa käsitellä ainoastaan silloin, kun on asiakas-tai hoitosuhde tai muu työtehtävään liittyvä suhde asiakkaaseen/potilaaseen.
- Rekisterinpitäjän on kerrottava rekisteröidyille henkilötietojen käsittelystä selkeästi ja ymmärrettävästi. Hyvinvointialueen nettisivuilta löytyy informointi asiakas-/potilastietojen käsittelystä (tietosuojaseloste).
- Hyvinvointialueelle on laadittu STM:n ohjeiden mukainen tietoturvasuunnitelma, joka sisältää yleiset tietoturvakäytännöt, käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt, käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt, Kanta-palvelujen käytön tietoturvakäytännöt, ym.
  - Tietoturvasuunnitelman liitteenä on asiakastiedon käytön valvontasuunnitelma (lokivalvontasuunnitelma)
- Potilastiedot arkistoituvat Kantaan vuodesta 2014 ja sosiaalihuollon tiedot marraskuusta 2024.
- Ensimmäiset onnistuneet vanhojen tietojen arkistoinnit Kantaan tehtiin vuoden 2024 lopussa.

4. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Tietotilinpäätös on yksi keino täyttää EU:n yleisen tietosuoja-asetuksen mukainen rekisterinpitäjän osoitusvelvollisuus (artikla 24, Rekisterinpitäjän vastuu).

- Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuoja-periaatteiden käytännön toteuttaminen dokumentoidaan.
- Osoitusvelvollisuuden toteuttamisen lisäksi tietotilinpäätös antaa tietosuojan tilannekuvan ja toimii tietosuojatyön kehittämisen välineenä, sisäisen ja ulkoisen valvonnan raporttina, johdon työvälineenä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan.
- Rekisterinpitäjän tulee osoittaa noudattavansa asetusta ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä. Rekisterinpitäjä vastaa osoitusvelvollisuuden toteuttamisesta.

4.1 Tietosuojan ja tietoturvallisuuden hallintamalli

Tietosuojan ja tietoturvallisuuden ohjausryhmä

- Ohjausryhmä linjaa ja kehittää tietoturvallisuutta sisäänrakennettuna kaikkeen toimintaa. Ohjausryhmä nimeää tietosuoja- ja tietoturvatyöryhmän, joka toimii tietosuojavastaavan ja tietoturvapäällikön tukena tietosuojan ja tietoturvan hallintamallin käytännön toteuttamisessa.

Tietosuojan ja tietoturvan työryhmä

- Tietosuoja- ja tietoturvatyöryhmän tehtävänä on valmistella organisaation tietosuojaa koskevaa ohjeistusta ja sisäisiä menettelyjä tietosuojan toteuttamiseksi sekä sen osoittamiseksi, että tietosuoja toteutuu toiminnassa.

Tietosuoja-/tietoturvatiimi, valvontayksikkö

- tietosuojavastaava
- tietosuoja-asiantuntijat
- tietoturvapäällikkö

4.2 Tietosuojavastaava

on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa.

Tietosuojavastaavan tehtäviä (GDPR):

- seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita.
- antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille.
- antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta.
- on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa.
- on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.

4.3 Tietosuojaa koskevat vaikutustenarvioinnit (DPIA)

Tietosuojaa koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä.

Arvioinnin on sisällettävä vähintään

- kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksesta
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä
- suunnitellut toimenpiteet riskeihin puuttumiseksi

Tuloksena syntyy näkemys tarvittavista hallintakeinoista, joita tarvitaan pienentämään riskitasoa ja varmistamaan asetuksen vaatimusten toteuttaminen.

Työkaluina käytössä

- alkukartoituslomake (tarvittaessa)
- vaikutustenarvioinnin työkalu (DPO365 sovellus tai TSV:n excel-taulukko)
- TSV ohje vaikutustenarvioinnista

Tietosuoja-arviointeja on tehty tähän mennessä hyvinvointialueella noin 30 kpl, näistä osa vielä kesken. Henkilötietoja sisältäviä järjestelmiä, joista asetus edellyttää arvioinnin tekoa, on noin 180 kpl.

4.4 Lokivalvonta

Asiakas- ja potilastietojen käytön valvonta perustuu asiakastietolakiin.

Tietojen käsittelyä valvotaan lokivalvontasuunnitelman mukaisesti. Lokitarkastus voidaan käynnistää rekisteröidyn, viranomaisen, asiakkaan tai yhteistyökumppanin pyynnöstä.

Mikäli lokiseurannan tai muun tietojen käsittelyn valvonnan perusteella todetaan, että tietoja on käsitelty lainsäädännön tai lupaehtojen vastaisesti, arvioidaan rikkeen vakavuus ja määrätään seuraamuksia.

Keskitetty lokienhallinta mahdollistaa paremman tilanneseurannan ja parantaa poikkeamienhallintaa. Vain osa järjestelmistä on keskitetyn lokiseurannan piirissä.

Rekisteröidyllä on asiakastietolain mukaan oikeus saada tieto, kuka on käsitellyt hänen tietojaan, mitä tietoja on käsitelty ja perusteet tietojen käsittelyyn. Tiedot on oikeus saada kahdelta edeltävältä vuodelta ilman erityisiä perusteita.

- Lokitarkastuksia tehtiin vuonna 2024 121 kpl (v.2023 144 kpl), ja väärinkäytös todettiin kolmessa tapauksessa.
- Systemaattista ja säännöllistä lokivalvontaa ei ole pystytty toteuttamaan, koska järjestelmät ovat vielä hajallaan, eikä niitä ole saatu integroitua keskitettyyn lokivalvontaan, jolloin nykyiset resurssit mahdollistaisivat paremman valvonnan.

4.5 Sopimukset ja hankinnat

Tietosuoja-asetus asettaa velvollisuuden sopia henkilötietojen käsittelystä erillisellä sopimuksella, kun joku muu (esim. palveluntuottaja) käsittelee tietoja rekisterinpitäjän puolesta/lukuun.

- Asetuksessa säädetään henkilötietojen käsittelysopimuksen minimisisällöstä, joka kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään.
- Tietosuoja-asetuksen artiklan 28 vaatimukset tättävät ehdot pitää sisällyttää kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja hyvinvointialueen lukuun.

Satakunnan hyvinvointialueella on henkilötietojen käsittelysopimuksesta (DPA) mallipohja, jota ensisijaisesti käytetään liitteenä.

Satakunnan hyvinvointialue on ottamassa käyttöön 2025 keväällä VM:n julkisten hankintojen tietoturvallisuus suositukset hankinnan kohteen ja toimittajan arviointiin sekä sopimusliitteen, jolla toimittaja sitoutuu toimittamaan palvelun suosituksen mukaisesti.

4.6 Koulutukset ja ohjeistus

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta.

- Organisatorisia toimenpiteitä ovat mm. koulutukset ja ohjeistukset työntekijöille.

Tietosuoja ja tietoturva on sisällytetty hyvinvointialueen perehdytyssuunnitelmaan

Kaikki Satakunnan hyvinvointialueen työntekijät on velvoitettu suorittamaan tietoturvan ja tietosuojan verkkokoulun (Granite) ne moduulit, jotka koskevat heidän työtehtäviään. Jokaisen moduulin (8) päätteeksi on tentti, joka tulee hyväksyttävästi suorittaa. .

- Tenttien suoritukset kirjautuvat koulutushallintajärjestelmään, josta esihenkilöillä on velvollisuus valvoa työntekijöidensa suorituksia.
- Koulutus suoritetaan kahden vuoden välein tai jos lainsäädännössä tapahtuu merkittäviä muutoksia, jotka vaikuttavat koulutukseen.
- Verkkokoulutus päivitettiin marraskuussa 2024, jonka jälkeen kaikki työntekijät suorittavat päivitetyn koulutuksen.

4.7 Koulutukset ja ohjeistus

Tietosuojaa ja henkilötietoja koskevia toimintaohjeita on pyritty päivittämään hyvinvointialueelle siirryttäessä ja niiden päivitys jatkuu edelleen.

Esihenkilön tulee uuden työntekijän perehdytyksessä huolehtia siitä, että tietosuoja tulee huomioiduksi ja jokaisen uuden työntekijän tulee suorittaa vaaditut tietoturva- ja tietosuojatentit.

Tietosuojaa ja tietoturvaa koskevat ohjeet on koottu IMS-järjestelmään. Ohjeiden julkaisut ja päivitykset tiedotetaan intranetissä sekä esihenkilöille sähköpostilla.

- Satanen intra-sivuilla on oma tietoturvan ja tietosuojan alasivusto, josta on linkkejä ohjeisiin. → Tietosuojan ja tietoturvatyöryhmän tavoitteena on parantaa sivuston näkyvyyttä

Satakunnan hyvinvointialue osallistui TAISTO-harjoitukseen vuosina 2023 ja 2024 sekä KYHA-harjoitukseen vuonna 2023 ja näistä kootaan kehittämiskohteita.

4.8 Tietoturva ja jatkuvuudenhallinta

Tietoturvapäällikön rooli ja vastuut

- Tietoturvapäällikkö valvoo hyvinvointialueen hallinnollisen ja teknisen tietoturvallisuuden toteutumista ja raportoi sen toteutumisesta
- Tietoturvapäällikkö vastaa tietoturvan tason arvioinnista, hallinnollisten ja kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietoisuuden editämisestä organisaatiossa, yleisestä konserninlaajuisesta tietoturvaohjeistamisesta ja –tiedottamisesta.
- Tietoturvapäällikkö toimii Tietosuojan ja tietoturvallisuuden ohajsuryhmän esittelijänä ja ohjausryhmän alaisen työryhmän puheenjohtajana.

Hyvinvointialueen yhtenäistä tietosuoja- ja tietoturvapolitiikkaa toteutetaan tietoturvasuunnitelmalla, joka ohjaa organisaatiota riittäviin ja yhdenmukaisiin tietoturva- ja tietosuojakäytäntöihin digiturvallisuuden varmistamiseksi.

4.9 Tietojärjestelmien häiriöt v. 2024

Satakunnan hyvinvointialueen käytössä olevien tietojärjestelmien ja perustietotekniikkapalveluiden osalta koettiin kategorisesti seuraavia häiriöitä.

- asiakas- ja potilastietojärjestelmien saatavuushäiriöitä (Terveys LifeCare, Sosiaali LifeCare, Pegasos)
- kuvantamisen ja laboratoriojärjestelmien häiriöitä
- tietojärjestelmien välillä tietojen siirtoon liittyviä häiriöitä
- Axel itseilmoittautumisjärjestelmään liittyvä häiriö
- sähköpostijärjestelmään liittyviä häiriöitä
- virtuaalityöpöytäpalvelujen saatavuushäiriö
- laajempia sekä yksittäisiin toimipisteisiin kohdistuvia tietoliikennehäiriöitä.

Hyvinvointialueen ICT-palvelut huolehtivat saatavuuden seurannasta ja mahdollisista reklamaatioista, jos sovittua palvelutasoa ei ole saavutettu.

- Kriittisen järjestelmien osalta on sovittu palvelutaso (SLA), jonka ylittymisestä on sovittu hyvitysmenettely.

4.10 Tieteellinen tutkimus

Kaikkiin Satakunnan hyvinvointialueella tehtäviin tieteellisiin tutkimuksiin ja opinnäytetöihin tarvitaan tutkimuslupa. Lupa tarvitaan aina, jos tutkimuksessa käytetään Satasairaalan potilaskertomustietoja tai potilasnäytteitä tai jos toteutetaan kyselyjä tai toimenpiteitä henkilökunnan tai potilaiden keskuudessa. Lupaa edellytetään myös muussa kuin tutkimukseen tai opinnäytteisiin liittyvässä toisiolain mukaisessa tietojen käytössä, esimerkiksi sisäisissä kehittämistöissä. Toisiolaissa säädetyt toissijaiset käyttötarkoitukset ovat:

- tieteellinen tutkimus
- tilastointi
- kehittämis- ja innovaatiotoiminta
- viranomaisohjaus ja -valvonta
- viranomaisten suunnittelu- ja selvitystehtävä
- opetus
- tietojohtaminen.

5. REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN

Tietosuoja-asetuksen mukainen rekisteröityjen informointi

- Henkilötietoja kerätään eri rekisterihin tietojen käyttötarkoituksen mukaan
- Rekisteröityjen informointi toteutetaan tietosuojaselosteilla, jotka on laadittu käyttötarkoitusten mukaisista tietovarannoista.
- Rekisterinpitäjän on toimitettava rekisteröidyille henkilötietojen käsittelyä koskevat tiedot.
- Tiedot on annettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.
- Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien toteuttamista.

Asiakas- ja potilastietojen tietosuojaseloste löytyy hyvinvointialueen internet-sivuilta, muiden tietosuojaselosteiden laatiminen on vielä kesken ja ne julkaistaan vuoden 2025 aikana.

- Tietosuojavastaava ja tietosuojatiimi tarkistaa ja huolehtii tietosuojaselosteiden päivittämisestä.
- Tietosuojaselosteista vastaa ko. toimiala ja rekistereillä on nimetyt yhteyshenkilöt.

5.1 Rekisteröidyn oikeudet

Rekisteröidyillä on tietosuoja-asetuksen mukaan oikeuksia liittyen omiin henkilötietoihinsa ja niiden käsittelyyn, kuten oikeus tietään käsitelläänkö hänen tietojaan, mitä tietoja käsitellään sekä pyytää häntä koskevat tiedot itselleen tai oikeus vaatia virheelliset henkilötiedot oikaistavaksi.

Tietosuoja-asetuksen mukaiset tietopyynnöt

- oikeus saada pääsy tietoihin, tarkastuspyynnöt
- oikeus tietojen oikaisemiseen, oikaisupyynnöt
- oikeus tietojen poistamiseen, poistopyynnöt (jos pyyntö perutunut suostumukseen)
- oikeus henkilötietojen käsittelyn rajoittamiseen
- oikeus vastustaa henkilötietojen käsittelyä
- oikeus riitauttaa automaattinen yksittäispäätös
- lakisääteisiin rekistereihin ei sovelleta tietojen poistamista, vastustamista, eikä myöskään käsittelyn rajoittamista, jos siitä aiheutuu vaaraa hoidolle.

Julkisuuslain mukaiset tietopyynnöt

Asiakastietolain mukaiset tietopyynnöt, lokitietopyyntö

5.2 Tietopyynnöt

Rekisteröityjen oikeuksista on tiedotettu hyvinvointialueen internet-sivuilla ja sieltä löytyy sähköisessä sekä tulostettavassa muodossa lomakkeet tietojen tarkistusta, kopioiden saantia ja korjausta varten sekä lomake lokitietopyynnölle.

- Potilaskertomuskopioiden käsittely on keskitetty hyvinvointialueen arkistoon, sosiaalihuollon asiakastietojen tietopyynnöt ohjataan arkistosta ko. vastuualueelle.
- Sähköisten asiakas- ja potilasasiakirjojen käyttöä seurataan ja valvotaan lokitietojen avulla ennalta määritellyn suunnitelman mukaisesti. Lokivalvonnan avulla pyritään ehkäisemään salassa pidettävien asiakastietojen lainvastaista ja asiatonta käyttöä.
  - Lokivalvonnasta huolehtii tietosuojatiimi ja käytössä on keskitetty LogMonitor-järjestelmä.
  - Mikäli asiakas- tai potilastietojärjestelmän lokivalvonnassa havaitaan väärinkäytöksiä, tietosuojavastaava pyytää asianomaiselta työntekijältä tai viranhaltijalta asian johdosta kirjallisen selvityksen, jonka perusteella tehdään päätös toimenpiteistä yhdessä esihenkilön kanssa.
- Julkisuuslain mukaan asianosaisella, jonka oikeutta, etua tai velvollisuutta asia koskee, on oikeus saada tieto muunkin kuin julkisen asiakirjan sisällöstä, jos se voi vaikuttaa hänen asiansa käsittelyyn. Pyynnöt lähetetään kirjaamoon, josta ne ohjataan oikealle taholle.

5.3 Tietopyynnöt v. 2023-2024

Rekisterinpitäjällä on velvollisuus helpottaa rekisteröidyn oikeuksien käyttämistä ja varmistaa oikeuksien toteutuminen määräajassa. Määräaika tarkastuspyynnöissä on kuukausi (tarvittaessa kahden kuukauden lisäaika, josta ilmoitetaan pyytäjälle) ja lokitietopyynnöissä kaksi kuukautta.

TIETOPYYNNÖT		pyynnöt 2023	pyynnöt 2024
Tarkastuspyynnöt (GDPR)	sos / terv. (kielt)	585 / 307	472 / 1191
Oikaisupyynnöt (GDPR)	yht (kielt)		159 (29)
Poistopyynnöt (GDPR)	yht (kielt)		?
Rajoittamispyynnöt (GDPR)	yht (kielt)	1	0
Vastustamispyynnöt (GDPR)	yht (kielt)		0
Kieltäytyminen autom. päätöksenteosta (GDPR)	yht (kielt)		0
Lokitietopyynnöt (AsiakastL)	yht (kielt)	144	121
Tietopyynnöt vainajasta (AsiakastL)	yht (kielt)		583
Tietopyynnöt häke (GDPR/HäkeL)	yht (kielt)		6
Julk.lain muk. pyynnöt salassapid.tiedosta	yht (kielt)		15
Vakuutusyht. ja viranomaisten tietopyynnöt*	yht (kielt)		n. 3400
Rekisterien väliset tietopyynnöt*	yht (kielt)	5531	1188
Toisiolain mukaiset tietopyynnöt	vastuualue/tkio	800	47

***muutos laskentatavassa**

5.4 Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti.

Tietoturvapoikkeamista ja -loukkauksista on henkilökuntaa ohjeistettu tekemään tietosuoja-/tietoturvailmoitus HaiPro-järjestelmään.

- HaiPro-tietoturvailmoituksia tehtiin 434 kpl vuonna 2024
  - 204 ilmoituksen riskiluokka on arvioitu kohtalaiseksi tai merkittäväksi
  - Tietoturvailmoituksista on voitu lisäksi tehdä asiakas-/potilasturvallisuusilmoitus ja/tai työturvallisuusilmoitus
  - Seurauksina tietoturvaloukkauksista on tiedon luottamuksellisuuden, eheyden, saatavuuden tai käytettävyyden vaarantuminen.
  - HaiPro-järjestelmän tietoturvapoikkeamailmoituksia käsittelevät esihenkilöt tai heidän valtuuttamat henkilöt sekä tietosuojatiimi.
  - Esihenkilöt huolehtivat siitä, että tietoturvaloukkaus tulee yksikön toiminnassa käsitellyksi ja selvitetyksi.
  - Tietojärjestelmiin liittyvät tietoturvaloukkaukset ohjataan teknisen ict-palvelun selvitettäväksi ja tarvittaessa 2M-IT:lle tai järjestelmätoimittajalle.

5.5 Tietoturvaloukkauksista ilmoittaminen

Jos henkilötietoihin kohdistuu tietoturvaloukkaus, jolla on suuri riski tietojen väärinkäytölle tai salassa pidettävän tiedon suojan rikkoutumiselle, tästä tulee tehdä ilmoitus tietosuojavaltuutetulle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on saanut tiedon tapahtuneesta.

Myös rekisteröidylle tulee yleensä ilmoittaa tietoturvaloukkauksesta, jos hänen tietoihinsa kohdistuu riskiä.

- Viranomaisilmoitukset tietosuojavaltuutetulle tekee tietosuojatiimi.
- Yksikön esihenkilön vastuulla on huolehtia tietoturvaloukkauksesta ilmoittamisesta rekisteröidylle.
- Viranomaisilmoituksia tietosuojaloukkauksista tehtiin 82 kpl ja 45 rekisteröidyille ilmoitettiin tietoturvaloukkauksesta.

5.6 Tietoturvailmoitukset

Tietoturvailmoitukset ja niistä tehdyt viranomaisilmoitukset ja ilmoitukset rekisteröidyille

	2023	2024
HaiPro tietoturvailmoitukset	373	434
ilmoitukset tietosuojavaltuutetulle	35	82
ilmoitukset rekisteröidylle		45

- Määrällisesti eniten tietoturvailmoituksia tehtiin tietojärjestelmiin, työasemiin ja tietoliikenneyhteyksiin liittyvistä häiriöistä
- Muut tyypillisimmät aihekokonaisuudet, joista tietoturvailmoituksia tehtiin
  - asiakas-/henkilötietoja annettu tai lähetetty väärälle vastaanottajalle eli sivulliselle
  - organisaation sisällä väärälle vastaanottajalle lähetetyt sähköpostiviestit tai potilastietojärjestelmässä lähetyt viestit
  - vääriin tulostimiin tulostetut asiakirjat/tiedostot

5.7 Valvontaviranomaisten selvitys- ja tietopyynnöt

Tietosuojavaltuutettu on kansallinen valvontaviranomainen joka valvoo tietosuojalainsäädännön noudattamista. Rekisterinpitäjä on velvollinen ilmoittamaan tietosuojavaltuutetulle tietoturvaloukkauksesta, jossa kohdistuu suuri riski henkilötietoon. Myös kansalainen voi tehdä ilmoituksen tietosuojavaltuutetulle, jos epäilee tietojaan käsitellyn tietosuojalainsäädännön vastaisesti.

- Tietosuojavaltuutetun selvityspyynnöt koskivat toimia, mihin rekisterinpitäjä on ryhtynyt tietoturvaloukkauksen johdosta tai miksi tietoja ei ole luovutettu tai korjattu.
- Hyvinvointialue teki vuonna 2024 yhden tietosuojan ennakkoarviointipyynnön tietosuojavaltuutetulle työntekijöiden rokotusmerkintöjen kirjaamiskäytännöistä henkilöstöhallinnon tietoihin. Tähän ei ole vielä saatu vastausta.
- Hallinto-oikeus, eduskunnan oikeusasiamies ja oikeuskansleri voivat pyytää selvitystä tai ottaa kantaa tietosuojaan liittyviin asioihin, jos rekisteröity on tehnyt kantelun.
- Savoa Partneriin liittyvässä tietoturvaloukkauksessa tietosuojavaltuutettu otti kantaa, että rekisteröidyille pitää asiasta ilmoittaa julkisella tiedonannolla. Muu asiaan liittyvä on vielä käsittelyn alla.
- Syksyllä 2023 tapahtuneesta Tena-tietomurrosta tietosuojavaltuutettu teki selvityspyynnön, johon on silloin vastattu. Tietosuojavaltuutetun ratkaisun mukaisesti kaikille rekisteröidyille ilmoitettiin henkilökohtaisella kirjeellä tietoturvaloukkauksesta (n. 8000 henk.)

6. ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN

- Tämä on ensimmäinen Satakunnan hyvinvointialueen tietotilinpäätös ja tämän sisältöä ja rakennetta jatkossa kehitetään.
- Tiedonhallintamallin rakenne on vuoden 2024 aikana saatu melko pitkälle valmiiksi, mutta työ jatkuu sisällön osalta.
- Tietosuojan ja tietoturvan dokumentteja on laadittu ja saatu osittain lain vaatimalle tasolle, mutta nämä vaativat vielä työtä ja jalkautusta, jotta sisäänrakennettu tietosuoja ja osoitusvelvollisuus toteutuu.
- Organisaatioiden yhdistyminen hyvinvointialueeksi on edellyttänyt erilaisten ohjeiden yhtenäistämistä ja tämä vielä kesken.
- Tietosuojatiimi yhdessä tietosuojan ja tietoturvan työryhmän kanssa toimii operatiivisena toimijana, ohjausryhmän ohjauksessa, tähän työhön tarvitaan myös johdon ja koko organisaation sitoutumista
- Tärkeänä tavoitteena on saada tietosuojatyö vakiinnutettua kaikkien toimintojen osaksi = **sisäänrakennettu tietosuoja**.

6.1 Tietosuojatyössä havaitut ongelmakohdat, kehittämistarpeet ja onnistumiset

- Tietosuojan vaikutustenarviointia (DPIA) ei ole vielä saatu juurrutettua toimintaan ja sen tekeminen aloitetaan usein liian myöhäisessä vaiheessa, jos ollenkaan. Riskienhallinta voi jäädä vajavaiseksi.
- Lokivalvonta on painottunut rekisteröityjen tietopyyntöjen toteuttamiseen ja niihin liittyvien epäilyjen ja ongelmien selvittelyyn, systemaattista ja säännöllista lokivalvontaa ei resurssien ja järestelmien hajanaisuuden vuoksi ole pystytty toteuttamaan. Tähän pyritään panostamaan vuonna 2025.
- Tietosuojan sisäänrakentamista hankintoihin ja sopimuksiin on pyritty kehittämään. Tähän on laadittu ohjeistusta ja kriteereitä, jotka pitää vielä jalkauttaa toimialueilla hankinnoista ja sopimuksista vastaaville.
- Tietosuojaan liittyviä ohjeita on pyritty tuottamaan ja parhaillaan on työn alla ohje asiakastietojen käsittelijöille tietojen luovutuksista. Kirjaamista ja sen oikeellisuutta on kehitetty, tällä on merkittävä vaikutus mm. tilastoinnin oikeellisuuteen.

6.2 Tietosuojatyössä havaitut ongelmakohdat, kehittämistarpeet ja onnistumiset

- Rekisteröityjen oikeudet toteutuvat kohtalaisesti, mutta esim. kopioiden saamisessa saattaa olla viivettä, jos tietoja joudutaan hakemaan monista eri tavalla järjestetyistä ja sijaitsevista arkistoista varsinkin sosiaalihuollon osalta. Näiden arkistojen kehittäminen ja keskittäminen on tarpeen.
- Jostain syystä terveydenhuollon kopiopyyntöjen määrä on merkittävästi noussut edellisestä vuodesta, sosiaalihuollon pyynnöissä on pientä vähenemistä.
- Hätäkeskuslain muutos on vaatinut paljon selvittelyä, kun hätäkeskuspuheluiden sote- ja pelastustietojen rekisterinpito määriteltiin hyvinvointialueelle vuoden 2024 alusta.
- Pakollisen Granite-verkkokoulutuksen lisäksi HaiPro-käsittelijöille on järjestetty koulutusta tietoturvailmoitusten käsittelyyn. Sosiaali- ja terveydenhuollon asiakastietolain mukaisissa tietojenvaihdon lakiperusteissa on koulutustarpeita. Henkilöstön tietosuojaosaamisessa on edelleen kehitettävää.

6.3 Tietosuojatyössä havaitut ongelmakohdat, kehittämistarpeet ja onnistumiset

- Tietoturvaloukkausten havaitsemissa ja ilmoittamisessa on lisääntymistä, mutta prosessi ei ole vielä kaikille tuttu. Näiden käsittelyssä ja riskien vakavuuden arvioinnissa rekisteröityjen näkökulmasta on vielä kehitettävää. HaiPro-tietoturvailmoitusten määrä on lisääntynyt vuodesta 2023.
  - Puutteita on havaittu asiakirjojen käsittelyssä ja luovutuksessa, asiakastietoja on lähetetty tai luovutettu väärille asiakkaille.
  - Asiakas-/potilastietoja on kirjattu väärille henkilöille, koska asiakas on valittu järjestelmästä nimen tai syntymäajan perusteella eikä henkilötunnuksella
  - Sähköpostin vastaanottajien valinnassa tulee virheitä, jolloin tietoja lähetetään väärälle taholle.
  - Samoin verkkotulostusvalinta saattaa olla virheellinen, jolloin asiakastietoja sisältävä tuloste menee väärään tulostimeen, jonka sijainti saattaa olla tietosuojariski.

6.4 Tietosuojatyössä havaitut ongelmakohdat, kehittämistarpeet ja onnistumiset

- Käyttöoikeusasetuksen mukaisen käyttäjähallinnan kehittäminen on ollut hidasta, koska asiakastietojärjestelmän vaatima panos on vienyt ison osan resurssista. Työ jatkuu käyttäjähallinnan ja käyttäjärekisterin osalta, henkilöresurssi tähän on käytössä kevään 2025.
- Erityisesti käyttäjähallinnan dokumentaatio tulee saada kuntoon ja vahvojen tunnusten käytön ja käyttöoikeuksien elinkaaren valvontaa tulisi tehostaa.
- EU:n ulkopuolinen tiedonsiirto ja ja Yhdysvaltojen välisen Privacy Shield –järjestelyt vaativat asiantuntijuuden lisäämistä.
- EU:n tekoälyasetus ja tuleva kansallinen lainsäädäntö tuo tarkempaa säätelyä tekoälyn käyttöön ja tämä vaatii perehtymistä asiaan. Ensimmäiset säädökset voimaan 2.2.2025.
- Tietosuojaan ja tietoturvaan tulee kiinnittää huomiota varhaisemmassa vaiheessa hankkeita ja projekteja sekä hankinnoissa ja sopimushallinnassa.
- Yleinen tietosuojatietous on kuitenkin kasvanut ja työntekijät ovat olleet enemmän yhteydessä tietosuojatiimiin näissä kysymyksissä.