Pohjois-Karjalan hyvinvointialue

Tietosuoja- ja tietoturvapolitiikka

Julkinen asiakirja

Käsitelty: Pohjois-Karjalan hyvinvointialueen tietosuojatyöryhmä 26.2.2026
Aluehallitus 12.5.2026 § 107

Sisällysluettelo

Versiohistoria

Päivämäärä	Kuvaus	Hyväksyntä
30.11.2022	Hyvinvointialueen tietosuoja- ja tietoturvapolitiikka hyvinvointialueen toiminnan käynnistyessä	Aluehallitus 30.11.2022 § 222
12.5.2026	Pohjois-Karjalan hyvinvointialueen tietosuoja- ja tietoturvapolitiikan kokonaispäivitys	Aluehallitus 12.5.2026 §

1 Johdanto

Tietosuoja- ja tietoturvapolitiikka on Pohjois-Karjalan hyvinvointialueen – Siun soten (jatkossa hyvinvointialue) aluehallituksen hyväksymä julkinen asiakirja, joka ohjaa tietosuojan ja tietoturvan ylläpitämistä ja kehittämistä. Tietosuoja- ja tietoturvapolitiikka koskee koko hyvinvointialuetta sekä sen koko henkilöstöä (työntekijät, viranhaltijat, johto, harjoittelijat, työllistetyt, siviilipalvelushenkilöt sekä luottamushenkilöt) kattaen kaikki automaattiset, manuaaliset, kirjalliset ja suulliset tietojenkäsittelytehtävät, ja sen tarkoituksena on sitouttaa hyvinvointialueen koko henkilöstö tietosuojan ja tietoturvan vaatimustenmukaiseen toteuttamiseen. Koko henkilöstöä sitoo vaitiolovelvollisuus (tietosuojalaki 1050/2018 35 §; laki viranomaisten toiminnan julkisuudesta 621/1999 22 §, 23 §, jälj. julkisuuslaki), jota noudatetaan palvelussuhteen aikana, vapaa-ajalla sekä palvelussuhteen päättymisen jälkeen. Tietosuoja ja tietoturva on toteutettava yhdenmukaisesti kaikissa työskentely-ympäristöissä, muun muassa erilaisissa toimitiloissa, etätyössä sekä työ-, koulutus- ja virkamatkoilla. Politiikka määrittelee periaatteet, tavoitteet, vastuut sekä seurannan ja valvonnan käytännöt, joilla varmistetaan yksityisyyden suoja, tiedon luottamuksellisuus, eheys ja turvallinen käsittely.

Hyvinvointialueen toiminnassa käsitellään järjestämistehtävien mukaisesti luottamuksellisia ja salassa pidettäviä tietoja, kuten sosiaali- ja terveydenhuollon asiakastietoja, pelastustoiminnan tietoja, henkilöstötietoja sekä muita lainsäädännön perusteella suojattavia tietoja. Suojattaviin tietoihin kuuluvat lisäksi muun muassa liikesalaisuudet, tutkimustiedot sekä turvallisuus- ja varautumisjärjestelyihin liittyvät kuvaukset. Hyvinvointialueen tehtävien toteuttaminen sekä toiminnan laatu ja turvallisuus edellyttävät, että tietosuoja ja tietoturva toteutuvat kaikissa olosuhteissa. Ne ovat keskeinen osa hyvinvointialueen kokonaisturvallisuutta sekä riskienhallinnan kokonaisuutta. Hyvinvointialue edellyttää politiikan mukaista toimintaa myös tytäryhtiöiltään, osakkuus- ja osaomistusyhtiöiltään, sidosryhmiltään sekä muilta yhteistyö- ja sopimuskumppaneilta. Näillä tahoilla tulee olla omaan toimintaansa soveltuvat tietosuojaan ja tietoturvaan liittyvät dokumentaatiot ja ohjeistukset, joiden toteutumisesta ja valvonnasta he vastaavat omien vastuu- ja käytännemalliensa mukaisesti. Lisäksi niiden on huolehdittava henkilöstönsä osaamisen varmistamista ja ylläpitämistä.

Tietosuoja ja tietoturva on huomioitava kaikessa tietojenkäsittelyssä tietoaineistojen ja tietojärjestelmien koko elinkaaren ajan (laki julkisen hallinnon tiedonhallinnasta 906/2019 13 §, jälj. tiedonhallintalaki). Tietosuoja ja tietoturva on siten otettava huomioon jo suunniteltaessa tietojen käsittelyä, aina tiedon arkistointiin tai hallittuun hävittämiseen saakka. Turvallinen ja laadukas tietojen käsittely edellyttää pitkäjänteistä ja riskiperusteista kehittämistä, jatkuvaa seurantaa sekä uhkiin varautumista. Tavoitteiden toteutumista tuetaan muun muassa riskien arvioinnilla, henkilöstön koulutuksella ja ohjeistuksella sekä sisäisellä valvonnalla. Henkilötiedot ja muu suojattava tieto turvataan riittävin hallinnollisin ja teknisin tietoturvakeinoin.

Muut hyvinvointialueen tietosuojasta ja tietoturvasta annetut ja näihin liittyvät suunnitelmat ja ohjeet perustuvat tietosuoja- ja tietoturvapolitiikkaan, ja näitä ylläpidetään ja päivitetään omina asiakirjoinaan. Sisältönsä mukaisesti määräytyy lisäksi muiden asiakirjojen julkisuus. Hyvinvointialue toimii tiedonhallintayksikkönä (tiedonhallintalaki 906/2019 2 § 1 mom kohta 2), jonka osalta esimerkiksi tiedonhallinnan vastuut kuvataan erillisissä tiedonhallintaa koskevissa suunnitelmissa.

Tietosuojaan ja tietoturvaan liittyvät asiat tulee olla lisäksi huomioituna muun muassa hyvinvointialueen riskienhallintaan, varautumiseen, sisäiseen valvontaan, omavalvontaan, asiakas- ja potilasturvallisuuden ja laadunhallintaan sekä laiteturvallisuuteen liittyvissä asiakirjoissa sekä sopimuksissa ja palvelusetelisääntökirjoissa. Tietoturva- ja tietosuojariskien hallinta on osa hyvinvointialueen riskienhallintaprosessia. Riskien hallinnassa sovelletaan myös hyvinvointialueen riskienhallinnasta annettuja ohjeita ja määräyksiä. Tietoturva- ja tietosuojariskeistä raportoidaan sisäisen valvonnan ja riskienhallinnan raportointikäytännön mukaisesti.

2 Keskeiset käsitteet ja ohjaavat säädökset

2.1 KESKEISET KÄSITTEET

Jokaisella on oikeus henkilötietojensa suojaan (Suomen perustuslaki 731/1999 10 §), ja henkilötietojen käsittelystä säädetään Euroopan unionin (EU) yleisessä tietosuoja-asetuksessa (EU 2016/679, jälj. tietosuoja-asetus). Tietosuoja turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Sen tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Tietoturva puolestaan kattaa ne hallinnolliset, tekniset ja toiminnalliset keinot, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus kaikissa olosuhteissa.

Tietosuoja- ja tietoturvapolitiikan ymmärtämisen ja soveltamisen tueksi on määritelty keskeiset käsitteet, perustuen voimassa olevaan lainsäädäntöön, viranomaisohjeisiin sekä yleisesti hyväksyttyihin määritelmiin. Keskeiset käsitteet on koottu tämän tietosuoja- ja tietoturvapolitiikan liitteeseen 1 (julkinen asiakirja).

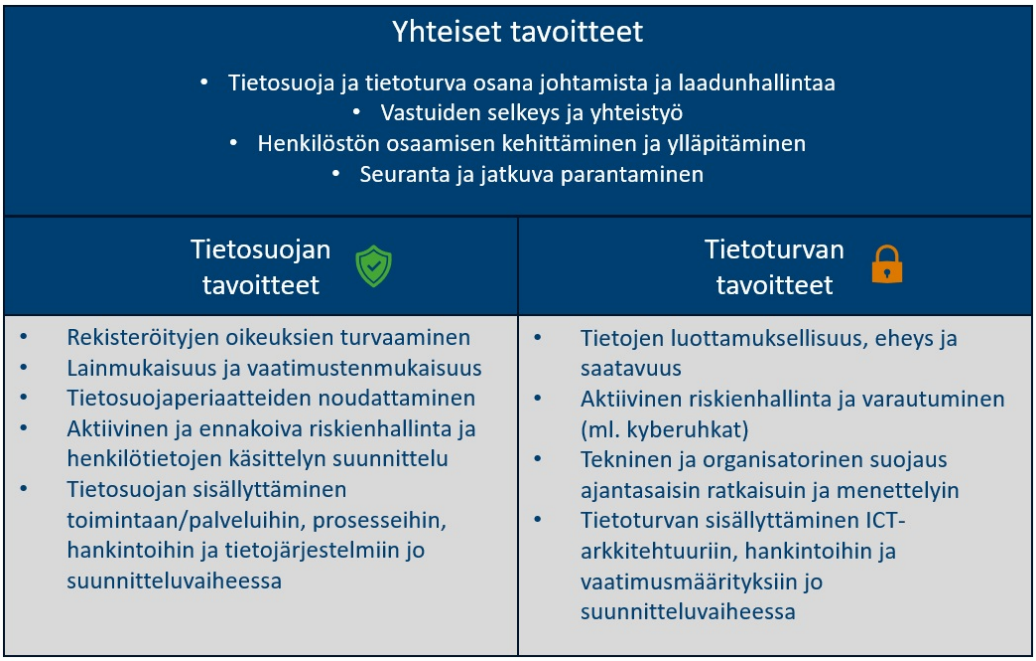
2.2 OHJAAVAT SÄÄDÖKSET

Tietosuojaa ja tietoturvaa ohjaavat voimassa oleva lainsäädäntö, viranomaismääräykset, ohjeet ja suositukset. Ohjauskokonaisuuden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä tietoturvallisuus kaikissa olosuhteissa.

Tietosuojaan ja tietoturvaan liittyvä ohjaus muodostuu eri tasoista, jotka etenevät Euroopan unionin (EU) tasoisesta sääntelystä kansalliseen lainsäädäntöön, kansallisiin viranomaismääräyksiin ja ohjeisiin sekä hyvinvointialueen omiin suunnitelmiin ja ohjeistuksiin. Sovellettavista säädöksistä ja ohjauksesta on koottu luettelo tämän tietosuoja- ja tietoturvapolitiikan liitteeseen 2 (julkinen asiakirja).

3 Tietosuojan ja tietoturvan keskeiset tavoitteet ja hallintatoimenpiteet

Hyvinvointialueen keskeiset tietosuojan ja tietoturvan tavoitteet tukevat sekä lakisääteisiä velvoitteita että hyvinvointialueen strategisia päämääriä. Tietosuoja ja tietoturva tukevat hyvinvointialueen palvelujen laatua, turvallisuutta ja luottamusta, ja niiden toteuttaminen edellyttää sekä teknisiä että organisatorisia ratkaisuja. Tavoitteiden kokonaisuus on havainnollistettu kuvassa 1.

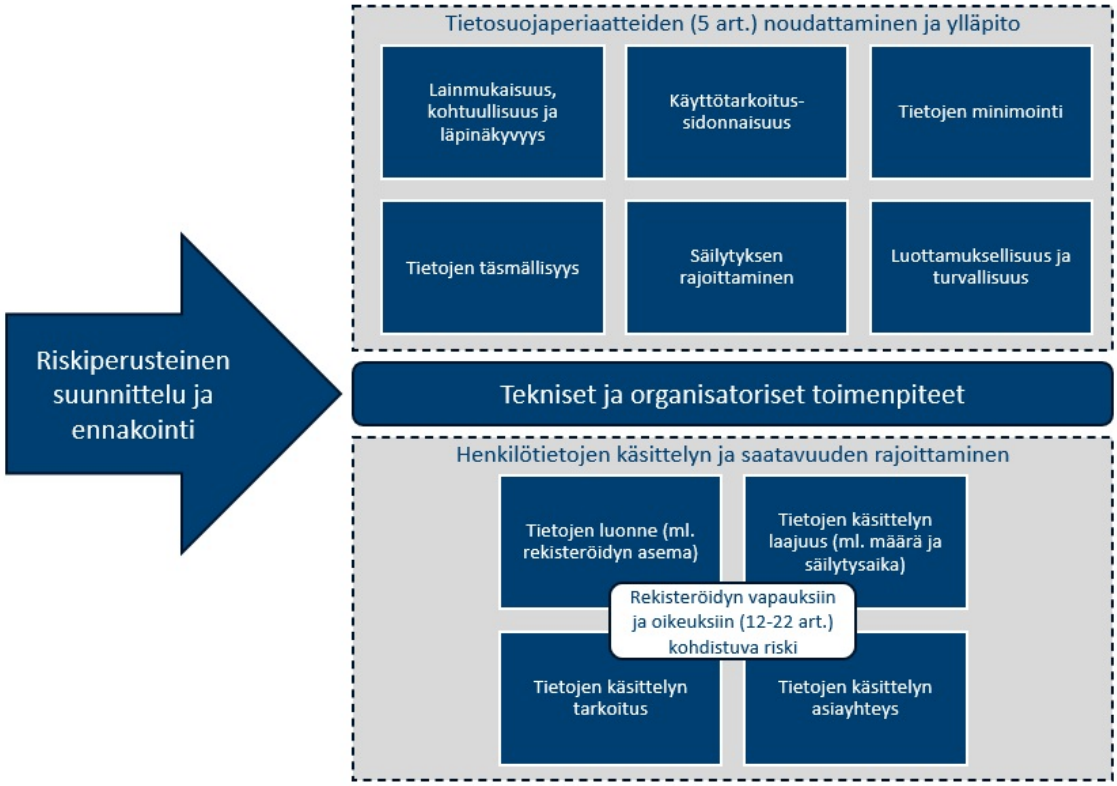


Kuva 1 Tietosuojan ja tietoturvan keskeiset tavoitteet

Sisäänrakennettu ja oletusarvoinen tietosuoja on yksi Euroopan unionin (EU) yleisen tietosuoja-asetuksen (EU 2016/679 25 art.) keskeisistä periaatteista ja hyvinvointialueelle rekisterinpitäjänä kuuluvista velvoitteista. Sisäänrakennettu tietosuoja tarkoittaa, että tietosuojaperiaatteet (5 art.) otetaan huomioon jo henkilötietojen käsittelyn suunnitteluvaiheessa. Tietosuoja sisällytetään osaksi toimintatapoja, henkilötietojen käsittelyprosesseja ja esimerkiksi tietojärjestelmiä alusta alkaen. Oletusarvoisen tietosuojan tarkoituksena on puolestaan varmistaa, että henkilötietoja käsitellään vain siinä laajuudessa kuin on välttämätöntä käsittelyn tarkoituksen kannalta. Tämä koskee muun muassa käsiteltävien henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja tietojen saatavuutta.

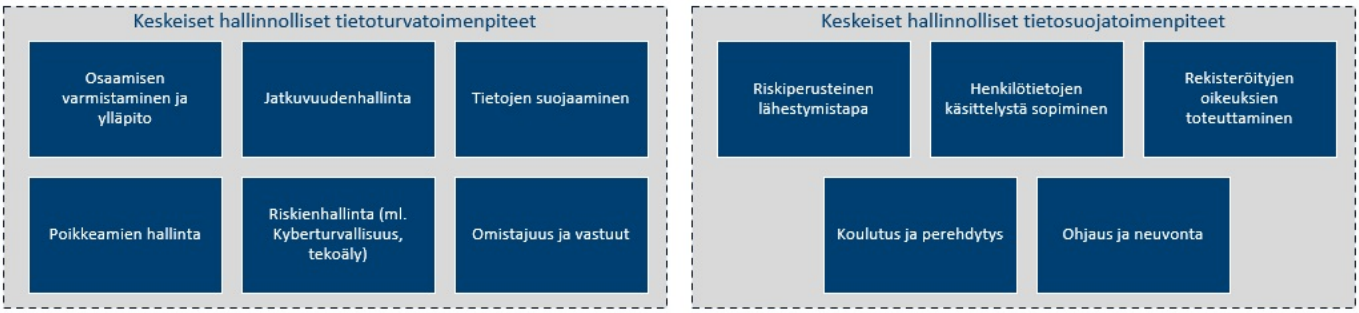
Hyvinvointialueen on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta (24 art.). Tietosuojaan liittyvien riskien arviointi on jatkuvaa toimintaa, ja toimenpiteiden riittävyyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Hyvinvointialueella on osoitusvelvollisuus riskiperusteisen lähestymistavan

noudattamisesta. Hyvinvointialueen henkilötietojen käsittelyn riskiperusteinen suunnittelu ja ennakoiva toiminta on havainnollistettu kuvassa 2.



Kuva 2 Henkilötietojen käsittelyn riskiperusteinen suunnittelu ja ennakointi

Toimenpiteillä pyritään vähentämään ja ennaltaehkäisemään tietosuoja- ja tietoturvariskejä, ja varmistamaan henkilöiden yksityisyydensuoja ja oikeusturva vaatimusten mukaisesti. Tietosuojan ja tietoturvan jatkuvaa ylläpitämistä toteutetaan hyvinvointialueella organisatoristen eli hallinnollisten ja teknisten hallintatoimenpiteiden avulla. Kyberturvallisuuden näkökulmasta toimenpitein suojataan tietojärjestelmät, verkot ja digitaalinen infrastruktuuri kyberuhkia vastaan. Siinä yhdistyvät sekä hallinnolliset että tekniset tietoturvatoimenpiteet. Keskeisiä hallinnollisia tietoturva- ja tietosuojatoimenpiteitä on havainnollistettu kuvassa 3.



Kuva 3 Keskeisimmät hallinnolliset tietoturva- ja tietosuojatoimenpiteet

Tietoturvatoimenpiteistä jatkuvuudenhallinta tarkoittaa kriittisten tietojärjestelmien ja tietoverkkojen keskeytyksetöntä toimintaa kaikissa tilanteissa siten, että niiden valtuudeton käyttö ja tahaton tai tahallinen tiedon tuhoaminen tai vääristyminen pyritään estämään sekä minimoimaan mahdolliset aiheutuvat vahingot. Hyvinvointialueen tiedot ja tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina toimenpitein ja käyttötarkoitusta rajaten. Tiedot, tietojärjestelmät ja laitteet on tarkoitettu vain työtehtävien hoitamiseen ja niiden muu käyttö ja hyödyntäminen on kielletty. Poikkeamatilanteista (ml. tietoturvaloukkaukset) ja niiden hallinnasta sekä riskienhallinnasta on hyvinvointialueella omat suunnitelmat ja ohjeistukset. Kaikille prosesseille, tietoaineistoille ja -varannoille, tietojärjestelmille ja laitteistoille sekä hyvinvointialueen oman ja ulkoistetun palvelutuotannon palveluille on määritelty omistajat ja vastuuhenkilöt. Tietoaineistojen ja tietovarantojen hallintaa ylläpidetään hyvinvointialueen tiedonohjaussuunnitelmassa sekä tietojärjestelmien hallintaa ylläpidetään tietojärjestelmäluettelossa (osa tiedonhallintamallia), jossa on määriteltynä lisäksi tietojärjestelmän kriittisyystaso. Tiedonluokittelun kattavuutta ja ajantasaisuutta edistetään aktiivisesti. Tietoaineistojen systemaattinen luokittelu on edellytys tekoälyratkaisujen laajamittaiselle ja turvalliselle käyttöönotolle, jotta voidaan varmistaa, ettei tekoäly käsittele tai yhdistele tietoja vastoin niiden käyttötarkoitusta tai suojaustasoa. Hallinnolliset tietoturvatoimenpiteet huomioidaan lisäksi hankinnoissa, hankkeissa ja projekteissa vaatimusten mukaisesti.

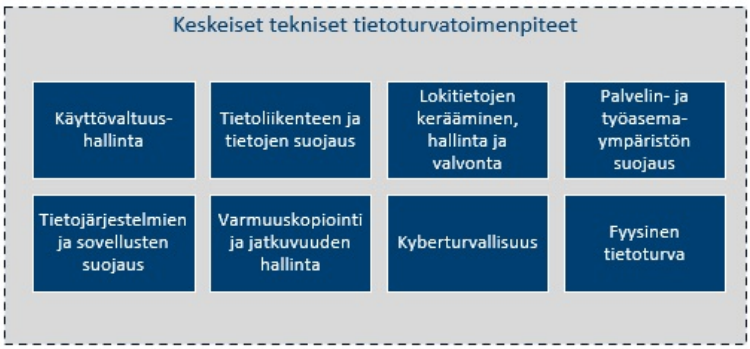
Tietosuojatoimenpiteiden riskiperusteinen lähestymistapa ohjaa henkilötietojen käsittelyä sekä uusien teknologioiden, kuten tekoälyn, käyttöönottoa hyvinvointialueella. Henkilötietojen käsittelystä laaditaan asianmukaiset tietosuojaa koskevat vaikutustenarvioinnit, mikäli käsittely aiheuttaa todennäköisesti korkeita riskejä rekisteröityjen oikeuksille ja vapauksille. Velvoite tehdä vaikutustenarviointi voi seurata suoraan tietosuoja-asetuksessa yksilöidyistä käsittelytilanteista, tietosuojaviranomaisen laatimaan luetteloon sisältyvästä käsittelytoimenpiteestä tai kansallisesta lainsäädännöstä. Rekisterinpitäjä voi kuitenkin hyödyntää vaikutustenarviointia milloin tahansa, kun se suunnittelee toimintoja, joissa on tarkoitus käsitellä henkilötietoja. Vaikutustenarviointiin määritellään riskiä pienentävät toimenpiteet ja tarvittaessa arvioinnista pyydetään ennakkokuulemista tietosuojavaltuutetulta. Tekoälyjärjestelmien osalta arvioidaan lisäksi niiden eettisyys, läpinäkyvyys, syrjimättömyys sekä Euroopan unionin (EU) tekoälyasetuksen (EU 2024/1689, jälj. tekoälyasetus) mukainen riskiluokitus. Erityistä huomiota kiinnitetään automatisoituun päätöksentekoon ja profilointiin varmistaen, että merkittävissä päätöksissä säilyy ihmisen tekemä valvonta.

Riskiperusteiseen lähestymistapaan liittyvät lisäksi henkilötietojen siirrot EU/ETA-alueiden ulkopuolelle, jossa keskiöön nousevat siirtoperusteiden määrittelyt. Hyvinvointialueen lukuun toimivien henkilötietojen käsittelijöiden (mm. palveluntuottajat) kanssa sovitaan henkilötietojen käsittelystä kirjallisesti osana sopimusta, hankintaa ja palvelusetelitoimintaa sekä tutkimus- ja kehittämishankkeita. Henkilötietojen käsittelijöiltä edellytetään vastuullista toimintaa sekä asianmukaisia toimenpiteitä tietojen käsittelyyn liittyvien riskien pienentämiseksi. Tekoälypalveluita hankittaessa sopimuksissa huomioidaan lisäksi tekoälymallien opetukseen käytettävän datan oikeudet, algoritmien toimintalogiikka sekä immateriaalioikeudet. Hallinnolliset tietosuojatoimenpiteet huomioidaan lisäksi hankinnoissa, hankkeissa ja projekteissa vaatimusten mukaisesti.

Tietosuojan ja tietoturvan hallintatoimenpiteistä keskeisin liittyy henkilöstön osaamisen varmistamiseen ja ylläpitoon, asianmukaisella ja ajantasaisella koulutuksella ja riittävällä perehdytyksellä. Lisäksi hyvinvointialueella turvataan riittävä asiantuntemus ja resurssi tietosuojan ja tietoturvan (ml. kyberturvallisuus ja tekoäly) ylläpitoon

ja kehittämiseen, joka on edellytys myös toimintaan liittyvälle ohjaukselle ja neuvonnalle, sidosryhmätyöskentelylle sekä rekisteröityjen oikeuksien toteuttamiselle.

Tietosuojan ja tietoturvan jatkuvaan ylläpitämiseen liittyvät tekniset hallintatoimenpiteet on havainnollistettu kuvassa 4.



Kuva 4 Keskeisimmät tekniset tietoturvatoimenpiteet

Käyttövaltuushallinnan tavoitteena on rajata käyttäjien pääsy vain työtehtävän edellyttämiin tietoihin ja tietojärjestelmiin sekä mahdollistaa säännöllinen käyttöoikeuksien tarkastus. Lisäksi käyttövaltuuksien tulee olla voimassa vain niin kauan kuin niitä tarvitaan työ- tai virkatehtävien hoitamiseen, ja niiden on päätyttävä palvelussuhteen päättyessä. Käyttöturvallisuutta ylläpidetään tietoliikenteen ja tietojen suojauksella, ICT-ratkaisujen toimivuuden valvonnalla (ml. lokitiedot) ja ylläpito- ja huoltotoiminnoilla, palvelin- ja työasemaympäristön suojauksella sekä tietojärjestelmien ja sovellusten suojauksella (ml. päivitykset) ja varmuuskopioilla. Teknisten tietoturvatoimenpiteiden osalta hyvinvointialueen sidosryhmätyöskentely ICT-palveluntuottajan kanssa on keskiössä. Tämä kattaa myös tekoälyjärjestelmien teknisen turvallisuuden varmistamisen, kuten mallien suojaamisen syöttöhäiriöiltä (tiedon myrkyttäminen) ja manipuloinnilta. Tietojärjestelmien ja sovelluspalveluiden saatavuudesta, käytettävyydestä, luotettavuudesta, hallinnoinnista ja valvonnasta sovitaan palveluntuottajan kanssa kirjallisesti. Tekniset tietoturvatoimenpiteet huomioidaan lisäksi hankinnoissa, hankkeissa ja projekteissa vaatimusten mukaisesti.

4 Tietosuojan ja tietoturvan vastuut hyvinvointialueella

Hyvinvointialue on julkisoikeudellinen itsehallinnollinen yhteisö (laki hyvinvointialueesta 611/2021 2 §). Hyvinvointialueella on järjestämisvastuu kulloinkin voimassa olevan lainsäädännön mukaisesti sille määrätyistä tehtävistä (laki hyvinvointialueesta 611/2021 6 §, 7 §). Vastuiden määrittely hyvinvointialueilla tulee tehdä

hallintosäännössä (laki hyvinvointialueesta 611/2021 95 §), joka on pätemisjärjestyksessä muihin dokumentteihin nähden ylempi vastuudokumentaatio.

Kaikessa henkilötietojen käsittelyssä korostuvat vastuukysymykset, jotka on järjestettävä tietosuojalainsäädännön mukaisesti riittävän tarkalla tasolla. Tässä tietosuoja- ja tietoturvapolitiikassa määritellään tietosuojaan ja tietoturvaan liittyvät vastuut, keskittyen henkilötietojen käsittelyyn ja yleiseen tietoturvallisuuteen. Määrittely on koottu tämän tietosuoja- ja tietoturvapolitikan liitteisiin 3 ja 4 (julkisia asiakirjoja).

5 Politiikan hyväksyminen ja ylläpito

Tietosuoja- ja tietoturvapolitiikan hyväksyy hyvinvointialueen aluehallitus. Tietosuoja- ja tietoturvapolitiikan ajantasaisuudesta ja säännöllisestä kerran vuodessa tapahtuvasta tarkastelusta vastaa hyvinvointialueen Tietosuoja- ja tietoturvatyöryhmä. Politiikka päivitetään kerran aluevaltuustokauden aikana tai mikäli hyvinvointialueen toimintaan liittyy merkittäviä muutoksia.

Liite 1 Keskeiset käsitteet

Käsite	Määritelmä	Lähde
Ennakkokuuleminen	Menettely, jolla rekisterinpitäjä ennen henkilötietojen käsittelyn aloittamista kuulee tietosuojaviranomaista. Ennakkokuuleminen on toteutettava mm. silloin, kun tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidylle, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi.	EU:n yleinen tietosuoja-asetus 2016/679, 36 art. Tietosuojavaltuutetun toimisto
Euroopan tietosuojaneuvosto (EDPB)	Euroopan unionin tietosuojaneuvosto (European Data Protection Board, EDPB), jonka asema, riippumattomuus ja tehtävät on säädetty tietosuoja-asetuksessa.	EU:n yleinen tietosuoja-asetus 2016/679, mm. VII luku 3. jakso
Henkilötieto ja erityiset henkilötietoryhmät	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity) liittyvät tiedot; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Erityisiin henkilötietoryhmiin kuuluvasta henkilötiedosta ilmenee henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettinen tai biometrinen tieto henkilön yksiselitteistä tunnistamista varten tai terveyttä koskeva tieto taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskeva tieto.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 1 EU:n yleinen tietosuoja-asetus 2016/679 9 art. kohta 1 Käsittelyä täsmennetään kansallisesti tietosuojalaissa (1050/2018 6 §).
Henkilötietojen käsittelijä	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijän suorittama käsittely on määritettävä sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan mm. käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 8 ja 28 art.
Henkilötietojen käsittely	Toiminto tai toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 2
Henkilötietojen tietoturvaloukkaus	Tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 12
Kyberriski	Poikkeaman aiheuttamien menetysten tai häiriön mahdollisuus, joka ilmaistaan menetyksen tai häiriön suuruuden ja poikkeaman toteutumisen todennäköisyyden yhdistelmänä.	Laki julkisen hallinnon tiedonhallinnasta 906/2019 2 § 1 mom. kohta 22

Kyberturvallisuus	Ne toimet, joiden seurauksena digitaalinen yhteiskunta kykenee varautumaan, tunnistamaan, torjumaan ja kestämään sähköisten ja verkotettujen järjestelmien häiriöitä ja niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin, toipumaan niistä sekä varmistamaan osaltaan kansallisen turvallisuuden, maanpuolustuksen ja huoltovarmuuden toimintaedellytykset.	Suomen Kyberturvallisuusstrategia 2024–2035
Kyberuhka	Tilanne, tapahtuma tai toiminta, joka toteutuessaan voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti. Merkittävällä kyberuhkalla tarkoitetaan kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti viranomaisen verkko- ja tietojärjestelmiin tai sen palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.	Laki julkisen hallinnon tiedonhallinnasta 906/2019 2 § 1 mom. kohta 20 ja kohta 21
Rekisteri	Mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 6
Rekisterinpitäjä	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.	EU:n yleinen tietosuoja-asetus 2016/679 4 art. kohta 7
Rekisteröity	Tunnistettu tai tunnistetavissa oleva luonnollinen henkilö, jota henkilötieto koskee.	Tietosuojavaltuutetun toimisto
Seloste käsittelytoimista	Rekisterinpitäjän ylläpitämä kirjallinen ja sähköisessä muodossa oleva seloste vastuullaan olevista käsittelytoimista. Myös henkilötietojen käsittelijän on ylläpidettävä omaa selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista. Seloste tulee tarvittaessa saattaa valvontaviranomaisen saataville.	EU:n yleinen tietosuoja-asetus 2016/679 30 art.
Tekoäly	Tekoäly laajana, monitulkintaisena ja muuttuvana teknologia-alueena ei mahdollista käsitteen pysyvää ja tarkkarajaista määritelmää. EU-tason sääntely kohdistuu tekoälyjärjestelmiin, joilla puolestaan on todellisia toiminnallisuuksia ja vaikutuksia. Kts. tekoälyjärjestelmä.	Ei virallista määritelmää.
Tekoälyjärjestelmä	Konepohjainen järjestelmä, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättelee vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin.	EU:n tekoälyasetus 2024/1689 3 art. kohta 1
Tietoaineisto	Asiakirjoista ja muista vastaavista tiedoista muodostuva tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus.	Laki julkisen hallinnon tiedonhallinnasta 906/2019 2 § 1 mom. kohta 5
Tietojärjestelmä	Tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely.	Laki julkisen hallinnon tiedonhallinnasta 906/2019, 2 § 3 kohta
Tietosuoja	Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena	Suomen perustuslaki 731/1999 10 § Tietosuojavaltuutetun toimisto

	on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.	
Tietosuojaa koskeva vaikutustenarviointi (DPIA)	Vaikutustenarviointi (Data Protection Impact Assessment, DPIA) kuvaa henkilötietojen käsittelyä, arvioi käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarvioinnin tavoitteena on arvioida, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä käsillä olevissa olosuhteissa. Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa. Vaikutustenarvioinnin laatiminen rekisterinpitäjän toimesta on edellytys mahdolliselle tietosuojavaltuutetun ennakkokuulemiselle.	EU:n yleinen tietosuoja-asetus 2016/679 84 resit. ja 35 art. Tietosuojavaltuutetun toimisto
Tietosuojaperiaatteet	Henkilötietojen käsittelyä koskevat periaatteet, joita on noudatettava aina henkilötietojen käsittelyssä, koko henkilötietojen käsittelyn elinkaaren ajan.	EU:n yleinen tietosuoja-asetus 2016/679 5 art.
Tietosuojavaltuutettu (TSV)	Tietosuoja-asetuksessa tarkoitettu kansallinen valvontaviranomainen, joka on toiminnassaan itsenäinen ja riippumaton, ja jonka tehtävistä säädetään tietosuoja-asetuksen 55–59 artiklassa. Tietosuojavaltuutettu edustaa Suomea Euroopan tietosuojaneuvostossa sekä laatii vuosittain tietosuoja-asetuksen 59 artiklassa tarkoitetun toimintakertomuksen, jota on pidettävä yleisesti saatavilla.	EU:n yleinen tietosuoja-asetus 2016/679 VI luku Tietosuojalaki 1050/2018 3. luku
Tietosuojavastaava	Tietosuojavastaava on riippumaton tietosuojalainsäädännön asiantuntija, joka mm. seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita sekä antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista organisaation johdolle ja henkilötietoja käsitteleville työntekijöille. Toimii rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa sekä toimii tietosuojavaltuutetun toimiston yhteyshenkilönä ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.	EU:n yleinen tietosuoja-asetus 2016/679 37 art. (nimittäminen), 38 art. (asema) ja 39 art. (tehtävät)
Tietoturva (tietoturvallisuus)	Tietoturvallisuudella eli tietoturvalla tarkoitetaan järjestelyjä ja toimenpiteitä, joiden avulla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tiedon saatavuudella tavoitellaan tiedon hyödynnettävyyttä haluttuna aikana. Tiedon eheydellä puolestaan tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa, ja tiedon luottamuksella estämään tiedon joutuminen sivullisille. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.	Kokonaisturvallisuuden sanasto, Sanastokeskus TSK ry (turvallisuuskomitea) Laki julkisen hallinnon tiedonhallinnasta 906/2019 2 § 1 mom. kohta 8
Tietovaranto	Viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettävä tietoaineistoja sisältävä kokonaisuus, jota käsitellään tietojärjestelmien avulla tai manuaalisesti.	Laki julkisen hallinnon tiedonhallinnasta 906/2019 2 § kohta 6

Liite 2 Tietosuojaa ja tietoturvaa ohjaavat säädökset ja muu ohjaus

Tietosuojaa ja tietoturvaa ohjataan EU-tasoisella säädännöllä, kansallisella lainsäädännöllä sekä muilla määräyksillä, ohjeilla ja suosituksilla. Tietosuoja- ja tietoturvapolitiikan hyväksymishetkellä voimassa oleva keskeinen lainsäädäntö:

- Arkistolaki 831/1994
- Elintarvikelaki 23/2006
- Eläinlääkintähuoltolaki 765/2009
- EU:n datanhallinta-asetus, EU 2022/868 (Data Governance Act, DGA)
- EU:n datasäädös, EU 2023/2854 (Data Act, DA)
- EU:n digimarkkinasäädös, EU 2022/1925 (Digital Markets Act, DMA)
- EU:n digipalveluasetus, EU 2022/2065 (Digital Services Act, DSA)
- EU:n tekoälyasetus, EU 2024/1689 (Artificial Intelligence Act, AIA tai AI Act)
- EU:n verkko- ja tietoturvadirektiivi, EU 2022/2555 (NIS2-direktiivi)
- EU:n yleinen tietosuoja-asetus, EU 2016/679 (GDPR)
- Hallintolaki 434/2003
- Jätelaki 646/2011
- Kyberturvallisuuslaki 124/2025
- Laki asiakkaan asemasta ja oikeuksista 812/2000
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki eräistä EU-direktiivissä säädetyistä lääkinnällisistä laitteista 629/2010
- Laki hyvinvointialueesta 611/2021
- Laki hätäkeskustoiminnasta 692/2010
- Laki julkisen hallinnon tiedonhallinnasta 906/2019
- Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015
- Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016
- Laki kunnan ja hyvinvointialueen viranhaltijasta 304/2003
- Laki lääkinnällisistä laitteista 719/2021
- Laki pelastustoimen järjestämisestä 613/2021
- Laki potilaan asemasta ja oikeuksista 785/1992
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023
- Laki sosiaali- ja terveydenhuollon järjestämisestä 612/2021
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä 552/2019
- Laki sosiaalihuollon ammattihenkilöstä 817/2015
- Laki sähköisen viestinnän palveluista 917/2014
- Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003

- Laki sähköisestä lääkemääräyksestä 61/2007
- Laki terveydenhuollon ammattihenkilöstä 559/1994
- Laki viranomaisen toiminnan julkisuudesta 621/1999
- Laki yksityisyyden suojasta työelämässä 759/2004
- Laki ympäristöterveydenhuollon yhteistoiminta-alueesta 410/2009
- Pelastuslaki 379/2011
- Perustuslaki 731/1999
- Rikoslaki 39/1889 (mm. 38 luku Tieto- ja viestintärikoksista)
- Sosiaali- ja terveysministeriön asetus sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 457/2024
- Sosiaalihuoltolaki 1301/2014
- Tekijänoikeuslaki 404/1961
- Terveydenhuoltolaki 1326/2010
- Terveydensuojelulaki 763/1994
- Tietosuojalaki 1050/2018
- Turvallisuusselvityslaki 726/2014
- Työsopimuslaki 55/2001
- Työterveyshuoltolaki 1383/2001
- Vahingonkorvauslaki 412/1974
- Valmiuslaki 1552/2011
- Ympäristönsuojelulaki 527/2014.

Lisäksi tietosuojaa ja tietoturvaa ohjaavia keskeisiä dokumentteja ovat mm.:

- Tietosuojavaltuutetun toimiston ohjeet ja linjaukset, jotka täydentävät tietosuoja-asetuksen ja tietosuojalain soveltamista
- Euroopan tietosuojaneuvoston ohjeet (EDPB) ja sitä edeltäneen EU:n tietosuojatyöryhmän ohjeet, siten kun niitä sovelletaan suhteessa uuteen tietosuojaneuvostoon.
- Tiedonhallintalautakunnan antamat suositukset ja ohjeet tiedonhallinnan toteuttamisesta julkisessa hallinnossa
- Sosiaali- ja terveysministeriön julkaisut (mm. oppaat, suositukset ja määräykset)
- Terveyden ja hyvinvoinnin laitoksen julkaisut (mm. oppaat, suositukset ja määräykset)
- Valtioneuvoston periaatepäätökset ja strategiat (mm. kansallinen kyberturvallisuusstrategia)
- Eduskunnan oikeusasiamiehen ja valtioneuvoston oikeuskanslerin sekä yleisten tuomioistuinten ratkaisut
- Kyberturvallisuuskeskuksen (Traficom) julkaisut (mm. tietoturvaohjeet, varoitukset ja arviointipalvelut)
- Valtiovarainministeriön julkaisut (mm. julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkri sekä generatiivisen tekoälyn hyödyntämisestä julkisessa hallinnossa).

Liite 3 Pohjois-Karjalan hyvinvointialueen rekisterien vastuuhenkilöiden tehtävät

Velvoite	Velvoitteen kuvaus
Dokumentointi- ja osoitusvelvoite	Rekisterin vastuuhenkilö pitää yllä vastuullaan olevan rekisterin osalta kirjallista, tietosuoja-asetuksen (30 artikla) mukaista selostetta käsittelytoimista. Seloste käsittelytoimista on hyvinvointialueen sisäinen asiakirja, kooten yhteen koko hyvinvointialueella suoritettavan henkilötietojen käsittelyn. Seloste käsittelytoimista on oltava sähköisessä muodossa, ja se on pyydettäessä esitettävä valvontaviranomaiselle. Rekisterin vastuuhenkilö huolehtii vastuullaan olevan rekisterin osalta tietosuoja-asetuksen (5 artikla) mukaisesta osoitusvelvollisuudesta ja sisäänrakennetun ja oletusarvoisen tietosuojan toteutumisesta (25 artikla). Osoitusvelvollisuus kattaa myös dokumentointivelvoitteen, jotta tietosuojaan ja henkilötietojen käsittelyyn liittyvät asiat (mm. sopimukset, ohjeistukset ja riskiarviot sekä tietoturvaloukkaukset) ja niiden käsittely toimenpiteineen voidaan tarvittaessa jälkikäteen osoittaa.
Henkilötietojen käsittelyn riskien arvioiminen ja tietosuojaa koskeva vaikutustenarviointi sekä ennakkokuuleminen	Rekisterin vastuuhenkilö varmistaa, että vastuullaan olevan rekisterin henkilötietojen käsittelyn riskit on arvioitu tietosuoja-asetuksen (24 artikla) mukaisesti ja käsittelyn turvallisuudesta (32 artikla) on huolehdittu. Mikäli rekisteröityjen oikeuksiin ja vapauksiin kohdistuu korkea riski, vastuuhenkilö varmistaa, että tietosuojaa koskeva vaikutustenarviointi (35 artikla) laaditaan ja riskeille määritellään hallintatoimenpiteet. Vaikutustenarviointi laaditaan hyvinvointialueen mallipohjalle. Mikäli jäännösriskit hallintatoimenpiteiden jälkeen jäävät korkeiksi, vastuuhenkilö käynnistää valvontaviranomaisen ennakkokuulemismenettelyn (36 artikla) konsultoiden juristia ja tietosuojavastaavaa ennen menettelyyn ryhtymistä.
Henkilötietojen käsittelystä sopimisen velvoite	Rekisterin vastuuhenkilö varmistaa, että vastuullaan olevaan rekisteriinsä liittyvästä henkilötietojen käsittelystä hyvinvointialueen lukuun sovitaan tietosuoja-asetuksen (28 artikla) mukaisesti. Sopiminen tulee tehdä kirjallisesti ja siitä tulee ilmetä rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja vastuut. Hyvinvointialueen omia henkilötietojen käsittelyn ehtoja sekä henkilötietojen käsittelytoimien kuvausta (ehtojen liite) käytetään hyvinvointialueella ensisijaisina sopimisasiakirjoina. Henkilötietojen käsittelystä sopimisesta vastaa hyvinvointialueella sopimuksesta tai palvelun hankkimisesta vastaava henkilö (viranhaltija), jonka velvoitteena on tarvittaessa konsultoida rekisterin vastuuhenkilöä henkilötietojen käsittelystä sovittaessa. Mikäli henkilötietojen käsittelystä sovitaan muilla kuin hyvinvointialueen henkilötietojen käsittelyn ehdoilla, on sen oltava aina hyvinvointialueella sopimuksesta tai palvelun hankkimisesta vastaavan henkilön (viranhaltija) päätös. Päätöksellä tarkoitetaan vastuuhenkilön harkittua ja arvioitua päätöstä siitä, että sopiminen voidaan tehdä muilla ehdoilla. Henkilön vastuulla on varmistua siitä, että henkilötietojen käsittelystä sopiminen toteutuu tietosuoja-asetuksen mukaisesti. Muiden ehtojen käyttäminen on myös tarvittaessa oltava perusteltavissa ja osoitettavissa jälkikäteen.
Informointivelvoite	Rekisterin vastuuhenkilö pitää yllä vastuullaan olevasta rekisteristä laatimaansa kirjallista ja sähköisessä muodossa julkaistua, tietosuoja-asetuksen (12–14 artikla) mukaista informointia. Informoinnin on oltava rekisteröityjen saatavilla, rekisteröityjen ryhmästä (mm. asiakkaat, potilaat, asukkaat, henkilöstö) riippuen, joko hyvinvointialueen verkkosivuilla ja/tai sisäisessä intrasivustossa. Tarvittaessa informoinnin kerroksellisuudesta huolehditaan (mm. suullinen läpikäynti).

	Informoinnissa on kerrottava henkilötietojen käsittelystä (ml. tarkoitus ja oikeusperuste) ja rekisteröidyn oikeuksista. Informointi tehdään pääsääntöisesti tietosuojaselosteella, joka laaditaan hyvinvointialueen mallipohjalle.
Rekisterin käyttötarkoituksen ja oikeusperusteen sekä käyttöoikeuksien määrittämisen velvoite	Rekisterin vastuuhenkilö määrittää ja hyväksyy vastuullaan olevan rekisterin henkilötietojen käsittelyn tarkoituksen, käsittelyn oikeusperusteen sekä rekisteriin liittyvien käyttöoikeuksien yleisperiaatteet. Lisäksi vastuuhenkilö laatii tarvittavat ohjeet rekisteriin liittyvästä tietojen käsittelystä, ja varmistaa, että käsittelyyn osallistuvat henkilöt ovat saaneet riittävän koulutuksen ja perehdytyksen tietosuojaan ja tietoturvaan liittyvistä asioista rekisterin osalta.
Rekisterin yhteyshenkilö	Rekisterin vastuuhenkilö nimeää vastuullaan olevalle rekisterille tarvittaessa yhteyshenkilön, jonka tehtävänä voi olla mm.: • rekisterin tietosuojaselosteen (informointi) valmistelu rekisterin vastuuhenkilölle • huolehtia tietosuojaselosteen (informoinnin) ajantasaisuudesta ja käynnistää päivitysmenettelyt tarvittaessa • toimia yhteyshenkilönä rekisteröidylle, joka haluaa käyttää oikeuksiaan • toimia yhteyshenkilönä, kun tietosuojavastaava pyytää omaan tehtäväänsä liittyviä tai valvontaviranomaisen pyytämiä selvityksiä tai tietoja rekisteristä • riskienarvioinnin valmistelu (24 artikla) ja korkean riskin tilanteissa tietosuojaa koskevan vaikutustenarvioinnin (35 artikla) valmistelu. Rekisterin yhteyshenkilö ei vastaa henkilötietoja sisältävästä rekisteristä, vaan tehtävä voi olla avustava ja valmisteleva asiantuntijatuki rekisterin vastuuhenkilölle kuuluvien tehtävien osalta. Rekisterin vastuuhenkilö vastaa siitä, että yhteyshenkilöllä on riittävät valmiudet toimia tehtävässä ja yhteyshenkilö saa tarvittaessa vastuuhenkilöltä ohjausta ja tukea tehtäviensä hoitamisessa.
Rekisteröityjen oikeuksien toteuttamisen velvoite	Rekisterin vastuuhenkilö varmistaa, että rekisteröidyillä on mahdollisuus käyttää tietosuoja-asetuksen (15–22 artikla) mukaisia oikeuksia, jotka riippuvat henkilötietojen käsittelyn perusteesta. Lisäksi vastuuhenkilö varmistaa, että oikeuksien käyttämisen määräaikoja (ilman aiheetonta viivytystä, mutta viimeistään 1 kk kuluessa pyynnön vastaanottamisesta) noudatetaan, ja tarvittaessa määräajan jatkamisesta (enintään 2 kk) sovitaan rekisteröidyn kanssa. Rekisterin vastuuhenkilö voi tarvittaessa konsultoida juristia ja/tai tietosuojavastaavaa ennen pyynnön toteuttamista.

Liite 4 Pohjois-Karjalan hyvinvointialueen tietosuoja- ja tietoturvajärjestelyjä koskevat vastuut

Tehtävä	Vastuu
Aluehallitus	Aluehallitus toimii EU:n yleisen tietosuoja-asetuksen (2016/679 4 artiklan 7 kohdan) mukaisena rekisterinpitäjänä. Aluehallituksen vastuut ja tehtävät on määritelty hyvinvointialueen hallintosäännössä, perustuen lakiin hyvinvointialueista (611/2021 43 §). Tietoturvan ja tietosuojan osalta vastuissa ja tehtävissä korostuvat mm. laatu, ohjaus, valvonta (ml. laillisuuden valvonta ja sisäinen valvonta), sisäisen tarkastuksen järjestäminen, riskienhallinta sekä viestintä ja tiedottaminen. Tehtävien hoitaminen edellyttää säännöllistä raportointia tietoturva- ja tietosuojariskeistä ja kehittämistoimista. Aluehallituksen jäsenillä ja varajäsenillä tulee olla riittävä perehtyneisyys tietosuojaan, tietoturvaan ja kyberturvallisuuteen sekä niitä koskeviin lainsäädännöllisiin velvoitteisiin ja riskienhallintaan.
Hyvinvointialuejohtaja	Hyvinvointialuejohtajan vastuut ja tehtävät on määritelty hyvinvointialueen hallintosäännössä. Tietoturvan ja tietosuojan osalta vastuissa ja tehtävissä korostuvat mm. toiminnan ja palvelujen yhteensovittaminen, sisäisen valvonnan ja tarkastuksen sekä riskienhallinnan asianmukainen järjestäminen sekä viestintään ja tiedottamiseen liittyvät asiat. Hyvinvointialuejohtaja nimeää hyvinvointialueen tietosuoja- ja tietoturvatyöryhmän sekä nimeää hyvinvointialueelle tietosuojavastaavan. Tietosuojavastaavan nimittämisestä, asemasta ja tehtävistä säädetty EU:n yleisessä tietosuoja-asetuksessa (2016/679 37–39 artikla). Tehtävien hoitaminen edellyttää säännöllistä raportointia tietoturva- ja tietosuojariskeistä ja kehittämistoimista. Hyvinvointialuejohtajalla tulee olla riittävä perehtyneisyys tietosuojaan, tietoturvaan ja kyberturvallisuuteen sekä niitä koskeviin lainsäädännöllisiin velvoitteisiin ja riskienhallintaan.
Rekisterin vastuuhenkilö	Henkilötietoja sisältävien rekistereiden vastuuhenkilöt määritellään hyvinvointialueen hallintosäännössä. Rekisterin vastuuhenkilöiden sekä mahdollisesti heidän nimeämien rekisterien yhteyshenkilöiden tehtävät on kuvattu tämän tietosuoja- ja tietoturvapolitiikan liitteessä 3 (julkinen asiakirja).
Jokainen esihenkilö	Esihenkilöillä tarkoitetaan kaikkia niitä henkilöitä, jotka toimivat työnantajan edustajana ja käyttävät tähän liittyvää työnjohdollista oikeutta. Vastuut toimi-, palvelu- tai vastuualueensa osalta: • vastaa oman alueensa tietoturvallisuudesta ja tietosuojasta lainsäädännön, viranomaisten antamien ohjeiden sekä hyvinvointialueen politiikkojen, periaatteiden, suunnitelmien ja ohjeiden mukaisesti • huolehtii, että alueensa jokainen työntekijä ja viranhaltija on asianmukaisesti perehdytetty tietoturva- ja tietosuoja-asioihin ja tarvittavat salassapito- ja käyttäjäsitoumukset on laadittu • huolehtii omalta sekä työntekijöidensä osalta hyvinvointialueen velvoittamien tietosuoja- ja tietoturvakoulutusten suorittamisesta ja suorituksen voimassaolosta, huomioiden lisäksi tehtäväkohtaiset erityiset tietosuojaan ja tietoturvaan liittyvät vaatimukset sekä työtehtävien

	hoitamiseen liittyvät käyttöoikeudet sekä oikeuksien voimassaolon päättäminen palvelussuhteen päättyessä • seuraa tietosuojan ja tietoturvan osaamisen tasoa alueellaan ja valvoo toiminnan laatua ja turvallisuutta sekä puuttuu havaitsemiinsa epäkohtiin • tukee toiminnallaan tietosuojan ja tietoturvan jatkuvaa ylläpitämistä ja kehittämistä, osana toiminnan laatua ja turvallisuutta, huomioiden myös toiminnan ja toimitilojen mahdolliset muutostilanteet ja niiden vaatimat järjestelyt • ilmoittaa ilman aiheetonta viivytystä havaitsemistaan tai tietoonsa saamistaan tietojen käsittelyyn liittyvistä poikkeamista ja tietoturvaloukkauksista myös läheltä piti -tilanteissa omalle esihenkilölleen ja lisäksi erillisen ohjeistuksen mukaisesti • ilmoittaa ilman aiheetonta viivytystä havaitsemistaan tai tietoonsa saamistaan tietosuojaan tai tietoturvaan liittyvistä puutteista tai kehittämiskohteista omalle esihenkilölleen ja lisäksi erillisen ohjeistuksen mukaisesti • ilmoittaa ilman aiheetonta viivytystä havaitsemistaan tai tietoonsa saamistaan tietosuojaan ja tietoturvaan liittyvistä merkittävistä riskeistä rekisterin vastuuhenkilölle ja tietosuojavastaavalle • osallistuu alueensa poikkeamatilanteiden selvittämiseen ja käsittelemiseen sekä riskiarvioon perustuvien tietosuoja- ja tietoturvatoimenpiteiden määrittelemiseen ja toteuttamiseen • huolehtii, että sijaisena toimivalla henkilöllä on tehtäviensä hoitamiseen välttämättömät tiedot ja käyttöoikeudet, ja sijainen perehdytetään tietosuojaan ja tietoturvaan liittyviin velvoitteisiin ennen sijaisuuden alkua. Lisäksi on varmistettava, että käyttöoikeuksien voimassaolo päätetään viipymättä palvelussuhteen tai sijaisuuden päättyessä. • ilmoittaa tietoturva- ja tietosuojarikkomuksista omalle esihenkilölleen, rekisterin vastuuhenkilölle ja tietosuojavastaavalle sekä vastaa henkilöstöhallinnollisen prosessin käynnistämisestä toimenpiteineen.
Jokainen hyvinvointialueen tietojen käsittelijä	Hyvinvointialueen tietojen käsittelijällä tarkoitetaan kaikkia niitä henkilöitä, jotka voidaan lukea hyvinvointialueen henkilöstöksi. Hyvinvointialueen tietojen käsittelijä voi olla esimerkiksi luottamushenkilö, viranhaltija, työntekijä, esihenkilö, opiskelija tai tutkija. Vastuut: • vastaa omalta osaltaan ja omassa toiminnassaan tietoturvallisuuden ja tietosuojan toteutumisesta • noudattaa tietojen käsittelyssä erityistä huolellisuutta, erityisesti henkilötietojen, luottamuksellisten ja salassa pidettävien tietojen osalta • suorittaa tietojen käsittelyn lainsäädännön, viranomaisten antamien ohjeiden sekä hyvinvointialueen tietoturva- ja tietosuojavaatimusten mukaisesti. Vaatimuksia on asetettu politiikoissa, periaatteissa, suunnitelmissa ja ohjeissa, joista jokaisen tietojen käsittelijän on oltava tietoinen. • kysyy epäselvissä asioissa neuvoa ja ohjausta ensisijaisesti omalta esihenkilöltään ja tarvittaessa muilta hyvinvointialueen viranhaltijoilta tai asiantuntijoilta • huolehtii hyvinvointialueen velvoittamien tietosuoja- ja tietoturvakoulutusten suorittamisesta ja suorituksen voimassaolosta • ilmoittaa ilman aiheetonta viivytystä havaitsemistaan tietojen käsittelyyn liittyvistä poikkeamista ja tietoturvaloukkauksista myös läheltä piti -tilanteissa omalle esihenkilölleen ja lisäksi erillisen ohjeistuksen mukaisesti • ilmoittaa ilman aiheetonta viivytystä havaitsemistaan tietosuojaan tai tietoturvaan liittyvistä puutteista tai kehittämiskohteista omalle esihenkilölleen ja lisäksi erillisen ohjeistuksen mukaisesti Kaikki toiminnassa tapahtuvat poikkeamat, tietoturvarikkomukset ja henkilötietojen tietoturvaloukkaukset käsitellään tapauskohtaisesti. Tahallinen tai törkeän huolimaton toiminta johtaa seuraamuksiin, jotka

	käsitellään henkilöstöhallinnollisin prosessein. Lisäksi tällainen toiminta voi johtaa tapauskohtaisesti myös rikosoikeudellisiin toimenpiteisiin.
Tietosuoja- ja tietoturvatyöryhmä	Tietosuoja- ja tietoturvatyöryhmän tavoitteena on suunnitella ja kehittää hyvinvointialueen tietosuojakäytäntöjä, tietoturvallista toimintaa sekä organisaation tietosuoja- ja tietoturvatyötä. Tässä työssä otetaan huomioon EU:n yleisen tietosuoja-asetuksen (2016/679), tietosuojalain (1050/2018) ja muun hyvinvointialueen toimintaa ohjaavan lainsäädännön toiminnalle asettamat vaatimukset ja velvoitteet. Tietosuoja- ja tietoturvatyöryhmässä käsitellään ajankohtaisia tietosuojaan ja tietoturvaan liittyviä teemoja, sekä näihin teemoihin liittyviä ajankohtaisia hankkeita ja projekteja. Lisäksi työryhmässä käsitellään hyvinvointialueen keskeisiä tietosuoja- ja tietoturvaohjeistuksia, sekä tehdään tarvittavia linjauksia tietosuojaan ja tietoturvaan liittyen. Työryhmän hyväksymä keskeinen toimintaohje on hyvinvointialueen tietosuoja- ja tietoturvakäsikirja, jota päivitetään säännöllisesti. Lisäksi työryhmä vastaa hyvinvointialueen tietosuoja- ja tietoturvapolitiikan ajantasaisuuden katselmoinnista vuosittain ja koordinoi päivitystyön tarvittaessa. Tietosuoja- ja tietoturvatyöryhmä tukee työllään hyvinvointialueen tietoturvallisuuden ja kyberturvallisuuden kehittymistä, suunnittelua sekä toimeenpanemista. Työryhmän nimeää hyvinvointialuejohtaja. Työryhmä tuottaa asiakas- ja potilasturvallisuuden sekä laadunhallinnan tilannekuvaa oman toimintansa osalta hyvinvointialueen omavalvonnan ja laadunhallinnan ohjausryhmälle, joka muodostaa kokonaiskuvan asiakas- ja potilasturvallisuudesta sekä laadusta.