Liite: Palveluntuottajaohjeen keskeiset muutokset, versio 3.0 -> 4.0

Vertailu perustuu julkaistuun versioon 3.0 (1.11.2024) ja julkaisuun menevään versioon 4.0 (2.11.2026). Liitteeseen on koottu sisällöllisesti merkittävät muutokset. Pelkkiä numeroinnin, kirjoitusasun ja rakenteen teknisiä muutoksia ei ole luetteloitu erikseen, ellei niillä ole vaikutusta ohjeen sisältöön tai soveltamiseen.

Yhteenveto

Versiossa 4.0 palveluntuottajan vastuita on täsmennetty erityisesti henkilöstön ja alihankkijoiden ohjauksessa, käyttöoikeuksissa, tilaajan tietojen käsittelyssä, poikkeamien hallinnassa, rekisteröidyn oikeuksien toteuttamisessa ja valvonnassa. Ohjeeseen on lisätty tekoälyn käyttöä koskeva luku ja itsearvioinnin tarkastuslista on rakennettu uudelleen palveluntuottajan johtamis-, teknisten ja tietosuojakontrollien näkökulmasta.

Keskeiset muutokset

Aihe / kohta	Muutos versiossa 4.0	Merkitys
Johdanto ja soveltamisala	Ohjeen yhteys hyväksyttyyn tietoturva- ja tietosuojapolitiikkaan on tuotu näkyväksi. Soveltamisalaa on laajennettu sopimuksen ja palvelusetelin lisäksi muihin järjestelyihin. Palveluntuottajan velvollisuus noudattaa sopimusta, henkilötietojen käsittelyn ehtoja, tilaajan ohjeita ja tätä ohjetta on täsmennetty. GDPR 28 artiklan viittaus on korjattu.	Vahvistaa ohjeen asemaa politiikan käytännön jalkautuksena ja selkeyttää käsittelijän velvoitteiden kokonaisuutta.
Käsittelymallit ja rekisterinpito	Lisätty kuvaus vaihtoehdoista, joissa palveluntuottaja käyttää hyvinvointialueen laitteita/järjestelmiä tai omia laitteita/järjestelmiä. Sosiaalipalvelujen rinnakkais- ja suoraliittymät on kuvattu. Sopimuksen ulkopuolisten palvelujen tietojen käsittelyä on täsmennetty: hyvinvointialueen rekisteritietoja ei saa hyödyntää näissä tilanteissa.	Tekee erilaiset tekniset ja toiminnalliset käsittelymallit näkyviksi ja erottaa tilaajan rekisterin käytön muusta palveluntuottajan toiminnasta.
Organisointi, osaaminen ja alihankinta	Palveluntuottajan vastuuta on laajennettu henkilöstön perehdytykseen, osaamisen ylläpitoon, alihankkijoiden ohjaamiseen sekä käyttöoikeuksien ajantasaisuuteen. Tilaajan käyttöoikeuksien muutos- ja poistotarpeista on ilmoitettava viipymättä.	Siirtää vastuun yksittäisen työntekijän ohjeistamisesta selkeämmin myös palveluntuottajaorganisaation johtamisvastuuksi.
Salassapito	Otsikkoon on lisätty hyväksikäyttökielto ja käsittelyn tarpeellisuus on sidottu kulloiseenkin työtehtävään.	Korostaa, ettei salassa pidettävää tietoa saa käyttää oman tai toisen hyödyn tai vahingon tarkoituksessa ja että käsittely on tarveperusteista.
Hyvinvointialueen laitteet ja tunnistautuminen	Laitteiden käyttötarkoitusta, turvallisia tietovälineitä, työskentely-ympäristöä ja käsittelypaikkoja on täsmennetty. Yksityiskohtainen 12 merkin salasanamalli on korvattu tilaajan voimassa olevilla tunnistautumis- ja salasanavaatimuksilla.	Tekee vaatimuksesta teknologianeutraalimman ja sitoo toiminnan tilaajan kulloinkin voimassa oleviin vaatimuksiin.

Aihe / kohta	Muutos versiossa 4.0	Merkitys
	Tunnistautumistietojen vaarantumisesta ilmoittaminen sekä käyttöoikeusmuutokset on lisätty.	
Palveluntuottajan oma käsittely-ympäristö	Palveluntuottajan vastuu omien laitteiden, järjestelmien, tietoliikenneyhteyksien, ylläpidon ja käyttöoikeuksien suojaamisesta on täsmennetty. Tilaajan tietoja saa käsitellä vain sopimuksen mukaiseen tarkoitukseen, tarpeellisessa laajuudessa ja hyväksytyissä ympäristöissä.	Vahvistaa tarkoitussidonnaisuutta, hyväksyttyjen käsittely-ympäristöjen käyttöä ja palveluntuottajan omaa suojausvastuuta.
Internet ja verkkoon liitettävät laitteet	Hyvinvointialueen verkkoon liitettäviä laitteita koskeva kielto on täsmennetty siten, että laitteista on sovittava hyvinvointialueen tietohallinnon kanssa.	Selkeyttää hyväksymismenettelyn periaatetta.
Sähköposti, kalastelu ja pikaviestimet	Kalastelu- ja vaarantumistilanteiden toimintaohjetta on laajennettu koskemaan tunnusten antamista, tiedostojen lataamista ja muita toimia. Pikaviestimissä painotus on muutettu tilaajan hyväksymiin viestintäkanaviin ja tietojen suojaustarpeeseen.	Selkeyttää toimintaa epäillyssä tunnusten vaarantumisessa ja sitoo viestintäkanavan valinnan tilaajan hyväksyntään.
Sosiaalinen media	Lisätty vaatimus siitä, etteivät tekstit, kuvat, videot, äänitallenteet tai niiden taustat saa paljastaa luottamuksellista tietoa tai turvallisuusjärjestelyjä vaarantavaa tietoa.	Laajentaa salassapidon käytännön soveltamista somejulkaisuihin.
Tekoälyn käyttö	Lisätty kokonaan uusi luku. Tilaajan tietoja ei saa käsitellä tekoälypalvelussa eikä käyttää mallin kouluttamiseen tai vastaavaan tarkoitukseen ilman tilaajan etukäteistä hyväksyntää.	Tuo tekoälyn käytön osaksi samoja tietoturva-, tietosuoja-, salassapito- ja tiedonhallintavaatimuksia kuin muun tietojenkäsittelyn.
Työympäristö ja fyysinen suojaus	Työpisteiden, näyttöjen, tulostamisen, asiakirjojen kuljettamisen ja keskustelujen suojaamista on täsmennetty. Henkilön oikeellisuuden varmistaminen on ulotettu myös etäyhteydellä käytävään keskusteluun.	Täydentää salassa pidettävän tiedon fyysistä ja käyttötilanteisiin liittyvää suojaamista.
Tietoturva- ja tietosuojapoikkeamat	Ilmoitusvelvollisuus on laajennettu havaitusta tai epäillystä poikkeamasta, joka koskee tai voi koskea tilaajan tietoja, järjestelmiä tai palvelua. Lisätty vahingon rajaaminen, selvitystietojen säilyttäminen, vaikutusten arviointi ja tilaajan avustaminen.	Muuttaa kohdan yleisestä loukkausilmoituksesta kattavammaksi poikkeamien hallintavelvoitteeksi.
Asiakas- ja potilastietojen käsittely	Erikoissairaanhoitoon siirtymistä koskenut yksittäinen esimerkki on korvattu yleisellä periaatteella: käsittely edellyttää asiakas-/potilassuhdetta, työtehtävää tai muuta lainmukaista perustetta ja käsittelyoikeus päättyy tarpeen päättyessä.	Yleistää käsittelyoikeuden perusteen ja tekee siitä sovellettavamman eri palvelutilanteisiin.
Asiakkaan ja potilaan oikeudet	Täsmennetty sote-palvelujen käsittelyperusteeksi rekisterinpitäjän lakisääteinen velvoite. Oikeuksien hakemisen ja henkilötietojen käsittelyn kuvausta on päivitetty. Lisätty palveluntuottajan velvollisuus avustaa tilaajaa rekisteröidyn oikeuksien toteuttamisessa eikä palveluntuottaja toteuta rekisterinpitäjälle kuuluvaa pyyntöä itsenäisesti ilman erillistä sopimista.	Selkeyttää rekisterinpitäjän ja käsittelijän työnjakoa rekisteröidyn oikeuksissa.
Valvonta ja seuraamukset	Lisätty palveluntuottajan velvollisuus antaa tilaajalle valvontaa varten tarvittavat tiedot ja selvitykset käyttöoikeuksista, lokeista sekä tietoturva- ja tietosuojavaatimuksista. Yksityiskohtaiset	Vahvistaa tilaajan valvontamahdollisuuksia ja tekee seuraamuksia koskevasta tekstistä

Aihe / kohta	Muutos versiossa 4.0	Merkitys
	rikosnimikkeiden rangaistusasteikot on korvattu yleisemmällä tapauskohtaisella kuvauksella.	yleisemmän ja ylläpidettävämmän.
Rakenne ja numerointi	Palveluntuottajan oman ympäristön käyttö on siirretty ennen Internet/sähköposti/some-lukua. Uusi tekoälyluku muuttaa myöhempien lukujen numerointia.	Parantaa rakennetta ja nostaa palveluntuottajan oman ympäristön sekä tekoälyn käsittelyn näkyvämmäksi.
Liite 1: itsearvioinnin tarkastuslista	Vanha yksittäisiin käyttäjätoimiin ja erillisiin GDPR-oikeuksiin painottunut tarkastuslista on korvattu palveluntuottajan itsearviointilistalla. Uusina teemoina ovat mm. johtaminen ja osaaminen, alihankinta, käyttöoikeudet, käsittely-ympäristö, tiedonsiirto, testaus, lokitus ja valvonta, jatkuvuus ja palautuminen, tekoäly sekä poikkeamat.	Muuttaa liitteen yleisestä muistilistasta systemaattisemmaksi palveluntuottajan kontrollien itsearvioinniksi ja kytkee sen politiikkaan, ohjeeseen ja sopimusvelvoitteisiin.

Tarkastuslistan uudistuminen

Version 3.0 tarkastuslista sisälsi erilliset tietoturva- ja tietosuojatoimenpiteiden osiot ja runsaasti käyttäjäkohtaisia ohjeita sekä yksittäisiä rekisteröidyn oikeuksia. Versiossa 4.0 tarkastuslista on jäsennetty palveluntuottajan hallinnollisiin, teknisiin ja tietosuojakontrolleihin. Samalla rekisteröidyn oikeuksia koskevat yksittäiset kyllä/ei-väittämät on korvattu palveluntuottajan avustamis- ja ohjausmenettelyä arvioivalla kontrollilla.

Huomio vertailun rajauksesta

Liite kuvaa versioiden 3.0 ja 4.0 väliset olennaiset sisällölliset muutokset. Asiakas- ja potilasasiakirjojen kirjaamista koskevista pitkistä osuuksista on nostettu esiin vain ne kohdat, joissa velvoite tai toimintaperiaate muuttuu. Muutoin säilynyt sisältö ei ole mukana muutosluettelossa.