KAINUUN
hyvinvointialue

Käyttölokien seuranta- ja valvontasuunnitelma

Kainuun hyvinvointialue

KAINUUN hyvinvointialue

Sisällysluettelo

1 Johdanto

Tässä suunnitelmassa kuvataan Kainuun hyvinvointialueen henkilörekisterien (potilas-, asiakas- ja muiden henkilörekisterien) sekä Kanta-palvelujen tietojen käsittelyn seurannan ja valvonnan perusteet, käytönvalvonnan roolit, käyttäjärekisteri ja valvonnan toteutus sekä väärinkäytösten seuraamukset.

2 Henkilötietojen käytönvalvonnan perusteet

Henkilötietojen käytönvalvonta on osa organisaation tietosuojan toteutumista. Tietosuojalla tarkoitetaan henkilötietojen suojaamista lain- sekä ohjeiden vastaiselta ja henkilöä vahingoittavalta käytöltä, käsittelemiseltä ja luovuttamiselta. Käyttölokitietojen valvonta on osa Kainuun hyvinvointialueen tietoturvatyötä. Sen valvonta tehdään lainsäädäntöön perustuen.

Henkilökunnalta edellytetään henkilö- ja potilastietojen käsittelyn osaamista. Organisaation johto on antanut henkilökunnalle kirjalliset ohjeet henkilö- ja potilastietojen käsittelyn periaatteista. Työntekijät ovat sitoutuneet noudattamaan sääntöjä allekirjoittamalla asiakas- ja potilasasiakirjojen salassapito- ja käyttäjäsitoumuksen. Henkilöstöä opastetaan henkilötietojen tietoturvalliseen käsittelyyn työhön perehdytysten, koulutusten ja ohjeistusten avulla, ja heitä tiedotetaan henkilötietojen käsittelyn valvonnasta ja väärinkäytösten seuraamuksista.

Käytönvalvonta perustuu rekisterinpitäjän suojausvelvollisuuteen. Euroopan parlamentin ja neuvoston asetuksen (EU:n tietosuoja-asetus) 2016/679 25 artiklan mukaisesti organisaation tulee huolehtia sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Tietosuoja-asetuksen 24 artiklan mukaisesti rekisterinpitäjän vastuulla on toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007, asiakastietolaki) 5 §:n mukaan:

”*Sosiaalihuollon ja terveydenhuollon palvelujen antajan tulee pitää rekisteriä omien asiakastietojärjestelmiensä ja asiakasrekisteriensä käyttäjistä sekä näiden käyttöoikeuksista. Palvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin. Käyttölokirekisteriin tallennetaan tieto käytetyistä asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja käytetään, asiakastietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta.*

Luovutuslokirekisteriin tallennetaan tieto luovutetuista asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja luovutetaan, asiakastietojenluovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta ja luovutusajankohdasta.”

Kainuun hyvinvointialue vastaa käyttö- ja luovutuslokirekisteristä ja Kansaneläkelaitos (Kela) vastaa tiedonhallintapalveluun tallennetun tiedon luovutuslokirekisteristä.

Lain sähköisestä lääkemääräyksestä (61/2007, eReseptilaki) 24 §:n mukaan terveydenhuollon toimintayksikön ja apteekin on omalta osaltaan seurattava ja valvottava, että reseptikeskuksessa olevia tietoja voivat katsella ja käsitellä vain tämän lain mukaan siihen oikeutetut ja, että tietojen katselu ja käsittely tapahtuu tässä laissa säädetyillä perusteilla.

Rekisterinpitäjän, toimintayksikön ja apteekin tulee oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin, jos joku on lainvastaisesti katsonut, käyttänyt tai luovuttanut reseptikeskuksessa olevia tietoja. Seurannan ja valvonnan toteuttamiseksi terveydenhuollon toimintayksiköllä ja apteekilla on oikeus saada Kelalta lokitiedot siltä osin, kuin asianomaisen toimintayksikön ja apteekin henkilökunta on katsellut ja käsitellyt reseptikeskuksessa olevia tietoja.

Asiakkaan oikeudesta lokitietoihin on erityisesti säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 18 §:ssä (28.3.204/250):

- asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten sosiaalihuollon ja terveydenhuollon palvelujen antajalta lokirekisterin perusteella tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja, sekä mikä on ollut käytön tai luovutuksen peruste. Asiakastietopyyntö on tehtävä kirjallisesti ja rekisterinpitäjän on toimitettava lokitiedot viivytyksettä ja maksutta.
- asiakkaalla on vastaava oikeus saada Kansaneläkelaitokselta tieto 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun tallennettujen ja sen kautta näytettävien tietojen luovuttamisesta organisaatioilta toiselle.
- asiakkaalla ei kuitenkaan ole oikeutta saada lokitietoja, jos lokitietojen luovuttajan tiedossa on, että lokitietojen antamisesta saattaisi aiheutua vakavaa vaaraa asiakkaan terveydelle tai hoidolle taikka jonkun muun oikeuksille
- kahta vuotta vanhempia lokitietoja ei ole oikeutta saada, jollei siihen ole erityistä syytä
- asiakas ei saa käyttää tai luovuttaa saamiaan lokitietoja edelleen muuhun tarkoitukseen
- jos asiakas pyytää toistamiseen saman ajanjakson lokitietoja, palvelujen antaja tai Kansaneläkelaitos voi periä lokitietojen antamisesta kohtuullisen korvauksen, joka ei saa ylittää tiedon antamisesta aiheutuvia välittömiä kustannuksia. Pääsystä lokitietoihin 19 §:ssä tarkoitetun katseluyhteyden avulla ei kuitenkaan saa periä erillistä maksua
- jos asiakas katsoo, että hänen asiakastietojaan on käytetty tai luovutettu ilman riittäviä perusteita, tietoja käyttäneen tai tietoja saaneen palvelujen antajan tai Kansaneläkelaitoksen tulee antaa asiakkaalle pyynnöstä selvitys tietojen käytön tai luovuttamisen perusteista

Yleisemmin on sovellettu julkisuuslain 11 §:n asianosaisen tiedonsaantisäännöstä, joka mahdollistaa myös salassa pidettävän tiedon saamisen. EU:n tietosuoja-asetuksen 15 artiklassa säädetty tarkastusoikeus ei tule kyseeseen, koska lokitietojen rekisteröity on käyttäjä/työntekijä, ei asiakas.

3 Käytönvalvonnan roolit

3.1 Rekisterinpitäjän rooli

Rekisterinpitäjän on huolehdittava siitä, että tietosuojalainsäädännön mukaisia tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Henkilötietojen käsittelyssä noudatettavia periaatteita ovat käyttötarkoitussidonnaisuus, tietojen minimointi, säilytyksen rajoittaminen, täsmällisyys, lainmukaisuus, kohtuullisuus sekä läpinäkyvyys, eheys ja luottamuksellisuus ja sisäänrakennettu ja oletusarvoinen tietosuoja.

Tietosuojaperiaatteiden mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- 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.

Käyttäjäkohtaista lokitusta ja siihen perustuvaa käytönvalvontaa voidaan pitää tietosuoja-asetuksen 5 artiklan mukaisena, asiallisesti perusteltuna rekisterinpitäjän toiminnan kannalta.

3.2 Työnantajan rooli

Työnantajat voivat ehkäistä laitonta käsittelyä muun muassa työtehtävien määrittelyn, tietojärjestelmään ja henkilötietojen käsittelyyn liittyvän ohjeistuksen, käyttäjä- ja salassapitositoumusten sekä valvonnasta tiedottamisen avulla. Nämä keinot eivät kuitenkaan poista laittoman käsittelyn mahdollisuutta, jolloin tarvitaan myös jälkikäteisiä keinoja varmistaa ja todentaa henkilötietojen käsittelyn lainmukaisuus.

Työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella (Yksityisyyden suojasta työelämässä annettu laki 3 §).

3.3 Käyttäjän/työntekijän rooli

Käyttäjän/työntekijän näkökulmasta on kyse työtehtäviä varten annettujen käyttöoikeuksien jälkikäteisestä valvonnasta, jossa lokituksen tuottama näyttö voi joko tukea tai kumota luvattoman käsittelyn epäilyjä. Näiltä osin on kyse käyttäjien oikeusturvasta suhteessa väitteisiin luvattomasta käsittelystä.

Työntekijä on vastuussa siitä, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos se ei ole noudattanut rekisterinpitäjän lainmukaista ohjeistusta.

3.4 Asiakkaan rooli ja oikeudet

Asiakkaan näkökulmasta kyse on henkilötietojen suojan todentamisesta ja toteuttamisesta.

Todentaminen tarkoittaa sen selvittämistä ja osoittamista, onko henkilötietoja käsitelty siten, että kyseeseen voisi tulla rikosoikeudellinen vastuu henkilötietojen suojasta (salassapitorikos tai henkilörekisteririkos). Mikäli henkilötietojen käsittely todetaan laittomaksi, on tietosuojan toteuttamisessa kyse niistä toimenpiteistä, joilla puututaan tällaiseen käsittelyyn ja ryhdytään korjaaviin toimenpiteisiin.

Asiakkaan oikeudet liittyvät rikos- ja vahingonkorvausoikeudelliseen vastuuseen. Keskeiset rikostunnusmerkistöt ovat salassapitorikos/-rikkomus ja henkilörekisteririkos/-rikkomus.

3.4.1 Vahingonkorvausoikeus

Tietosuoja-asetuksen 82 artiklan mukaan henkilöllä, jolle on aiheutunut tietosuoja-asetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta. Käsittelijä on vastuussa vahingosta, jos hän ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos hän ei ole noudattanut rekisterinpitäjän lainmukaista ohjeistusta.

Jotta asiakas voisi käyttää tällaisia oikeuksiaan, on hänellä oltava tieto näistä oikeuksista ja tästä menettelystä.

3.5 Tietosuojavastaavan rooli

Tietosuojavastaavan tehtävänä on asiantuntijana auttaa johtoa velvoitteittensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutuksen toteutukseen.

Tietosuojavastaavan tehtävänä on seurata ja valvoa henkilötietojen käsittelyä ja suojausmenettelyä, tukea ja ohjata henkilökuntaa ja rekisteröityjä tietosuoja-asioissa, toimia yhdyssiteenä valvontaviranomaisiin sekä raportoida johdolle tietosuojan tilasta ja kehittämistarpeista.

Tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä ja ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa seuranta- ja valvontasuunnitelman mukaisesti. Tämän lisäksi suoritetaan valvontaa selvityspyyntöön perustuen.

3.6 Esimiehen rooli

Esimiehet osallistuvat lokitietojen tulkintaan ja arviointiin.

He voivat tehdä valvontapyyntöjä alaisistaan, osallistua kuulemistilaisuuksiin ja antaa varoituksen tai huomautuksen tarvittaessa. Esimiesten tulee myös aloittaa palvelussuhteen päättämistoimenpiteet, mikäli säännösten vastainen toiminta sitä edellyttää.

3.7 Lakimiehen rooli

Lakimies osallistuu lokitietojen tulkintaan ja arviointiin ja antaa suosituksia.

3.8 Järjestelmäasiantuntijan/ tiedonhallinnan suunnittelijan rooli

Järjestelmävastaavat ajavat lokitiedon pyydetystä järjestelmästä. Lokitiedon tulkintaan ja arviointiin osallistuu järjestelmäasiantuntijoiden lisäksi tiedonhallinnan suunnittelija.

4 Käyttäjärekisteri

Kainuun hyvinvointialueen tietoturva- ja tietosuojapolitiikan mukaisesti tietojärjestelmien käyttäjistä pidetään käyttäjähallintarekisteriä, jota käytetään rekisterien käyttöoikeuksien ja käyttäjäroolin määrittämiseen, asiattoman käytön etsimiseen, asiallisen käytön todentamiseen, epäiltyjen väärinkäyttötapausten selvittämiseen sekä asiakkaan tai potilaan tiedonsaantioikeuden toteuttamiseen.

Käyttäjähallintarekisteri perustuu tietosuoja-asetuksen (679/2016), lain potilaan asemasta ja oikeuksista (785/1992), lain sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000), lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), lain viranomaisen toiminnan julkisuudesta (621/1999), sosiaali- ja terveysministeriön asetuksen potilasasiakirjoista (298/2009) sekä lain yksityisyyden suojasta työelämässä (759/2004) säännöksiin, joissa kuvataan rekisterinpitäjän velvollisuutta suojata salassa pidettäviä tietoja, potilasta tai asiakkaan asiaa hoitavan oikeus käsitellä henkilöasiakirjoja, velvollisuus kerätä tietoja henkilötietorekisterin tietojen käsittelystä sekä velvollisuus antaa tietoja rekisteröidylle hänen tietojensa käsittelystä.

Käyttäjähallintarekisteri on looginen kokonaisuus, joka koostuu käyttäjien ja heidän käyttöoikeuksiensa rekisteristä sekä tiedonkäsittelyn rekistereistä, joita ovat käyttölokirekisteri ja luovutuslokirekisteri. Palvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin.

Käyttölokirekisteriin tallennetaan tieto käytetyistä asiakastiedoista, asiakastietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta. Luovutuslokirekisteriin tallennetaan tieto luovutetuista asiakastiedoista, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta ja luovutusajankohdasta.

Terveydenhuollon palvelujen antajien potilasasiakirjatietojen luovuttamista koskevat lokitiedot tallennetaan valtakunnalliseen arkistointipalveluun. Organisaatio saa lokitiedot tiedonhallintapalvelusta kirjallisella vapaamuotoisella pyynnöllä.

Koska lokitietoja saavat käyttää vain ne henkilöt, joiden työtehtäviin kuuluu vastata tietosuojan ja sen valvonnan toteuttamisesta, on käyttölokirekisteriin pääsy rajoitettu henkilöille, joiden työtehtäviin se on määritelty.

5 Käytönvalvonta

5.1 Lokivalvontaprosessi

Valvonta tapahtuu seuraavista lähtökohdista:

- Asiakaslähtöinen eli asiakas itse tekee valvontapyynnön.
- Viranomaislähtöinen eli poliisi tai valvova viranomainen (AVI) tekee valvontapyynnön
- Esimies tekee valvontapyynnön
- Satunnaisotantavalvonta

Lokivalvontaprosessin käytännön kulku sekä satunnaisotantavalvontaan että selvityspyyntöön perustuvassa valvonnassa on kuvattu liitteessä 1.

Rekisteröidyn tiedonsaantioikeuden käyttämiseen on erilliset lomakkeet: selvityspyyntö potilas/asiakastietojen käsittelystä ja potilas/asiakastietojen käyttölokin tietopyyntö, jotka osoitetaan tietosuojavastaavalle. Lokitiedon tulkinnan ja arvioinnin tekevät järjestelmävastaavat, tiedonhallinnan suunnittelija ja tietosuojavastaava. Mahdollisesta jatkoselvittelystä ja toimenpiteistä vastaa tietosuojavastaava.

Tietojärjestelmien tietojen käsittelyn jälkikäteisvalvonta tapahtuu pääasiassa perusjärjestelmien lokitietojen perusteella. Valvonnassa tarkastetaan asiakirjojen avaukset, katselut, tallennukset, ajankohta, aikaväli sekä tietojen käytön syvyys. Lokitietoja voidaan lisäksi verrata esim. vastaaviin työaikatietoihin tai asiointitietoihin. Lokivalvonnan lisäksi tarkkaillaan varmennekorttien asianmukaista käyttöä.

5.2 Selvityspyyntöön perustuva valvonta

Kun rekisteröity, viranomainen tai valvontaviranomainen tekee rekisterinpitäjälle käyttölokirekisterin selvityspyynnön rekisteriin tallennettujen tietojen käytöstä, käynnistyy selvitysprosessi tietosuojavastaavan toimesta liitteen 1 mukaisesti.

Selvitystyön perusteella tietosuojavastaava antaa pyytäjälle kirjallisen selvityksen tietojen käytöstä ja käytön perusteista.

Jos selvityspyynnön esittää kansallisen rekisterin rekisterinpitäjä (esim. Reseptikeskuksen osalta Kela), tietosuojavastaava antaa kirjallisen selvityksen tietojen käsittelystä organisaation sisällä kyseisen rekisterin vastuuhenkilölle, joka laatii rekisteröidylle vastauksen.

5.3 Satunnaisotantavalvonta

Satunnaisotantavalvontaa toteutetaan noin neljä (4) kertaa vuodessa mm. seuraavilla valvontatoimenpiteillä:

- valitaan lokitiedostoajon kohteeksi satunnaisotanta työntekijöitä maksimissaan viikon ajalta. Ilmenneistä väärinkäytöksistä ilmoitetaan asiakkaalle.

- valitaan lokitiedostoajon kohteeksi satunnaisotanta asiakkaita/potilaita (2 kpl molempia). Lokiajo ajetaan pistokokeena esim. viikon ajalta lokiajopyynnön päivämäärästä ja ilmenneistä väärinkäytöksistä ilmoitetaan asiakkaalle.

- valitaan lokitiedostoajon kohteeksi henkilöitä, jotka ovat olleet julkisuudessa/mediassa tai joiden tiedetään olleen hoidossa/asiakassuhteessa organisaatioon ja joilla on korkeampi riski joutua rekisteritietojen luvattoman käytön kohteeksi. Lokitieto ajetaan hoidon tai palvelutapahtumien ajalta. Ilmenneistä väärinkäytöksistä ilmoitetaan asiakkaalle.

6 Käytönvalvonnan kulku

6.1 Lokien tarkastaminen ja tulkinta

Lokien tarkastaminen ja tulkinta tehdään prosessikuvauksen (liite1 ja 2) mukaisesti. Lokien tarkastamisessa ja tulkinnassa tulee esille, onko tietojen käyttö perustunut asiakas-/potilassuhteeseen ja onko se ollut työtehtävien suorittamisen kannalta perusteltua. Lokitietojen tarkastamisen jälkeen lokiraportit toimitetaan kirjallisena tietosuojavastaavalle.

6.2 Selvityksen pyytäminen työntekijältä

Jos lokitiedostoajojen tarkastamisessa on tullut esille epäily, että asiakkaan tiedoissa on käyty aiheettomasti, tietosuojavastaava pyytää työntekijältä kirjallisen selvityksen rekisterin käytön perusteista.

Hallintolain 32 §:ssä säädetään, että selvityspyynnössä on yksilöitävä, mistä erityisistä seikoista selvitystä pyydetään. Selvityksen antamiselle on asetettava riittävä määräaika, jos selvityspyyntö koskee asiakirjan täydentämistä, selvityksen antamista tai selvityksen esittämistä. Määräaikaa asettaessa on huomioitava, että esittäminen voi edellyttää erityisiä selvitystoimia, joihin kuuluva kohtuullinen aika on otettava huomioon.

6.3 Selvityksen antaminen tietosuojavastaavalle

Työntekijän tulee palauttaa kirjallinen selvitys tietojen käytöstä tietosuojavastaavalle, joka toimittaa tarvittavat asiakirjat henkilön esimiehelle. Annettujen kirjallisten selvitysten, lokitietojen ja tarkastuksen sekä kannanottojen perusteella tehdään ratkaisu, onko kyseessä ollut perusteltu käyttö. Väärinkäytön ilmetessä tai epäselvissä tapauksissa kannanottoa pyydetään myös organisaation lakimieheltä.

6.4 Kuulemistilaisuus

Työntekijän kuuleminen toteutetaan siten, että hänelle annetaan kuulemisilmoitus, jossa ilmoitetaan kuulemisen tarkoitus ja selvityksen antamiselle varattu määräaika. Asianosaiselle on toimitettava kuulemisen kohteena olevat asiakirjat alkuperäisinä tai jäljennöksinä, taikka varattava muutoin tilaisuus tutustua niihin (HL 36 §). Jos päätösratkaisu perustuisi asiakirjoihin, joihin asianomainen ei ole voinut tutustua ja joihin hän ei ole voinut esittää kantaansa, menettelyä ei voitaisi pitää tasapuolisena.

Kuulemisen yhteydessä pyydettävän selvityksen antamiselle voidaan asettaa määräaika, jonka aikana henkilö voi tutustua asiaan sekä muodostaa siitä oman perustellun kannanottonsa. Asianomaiselle on ilmoitettava, ettei määräajan noudattamatta jättäminen estä asian ratkaisemista ja määräaikaa voidaan pyynnöstä pidentää, jos se on tarpeen asian selvittämiseksi (HL 33 §).

Kuuleminen toteutetaan siten, että esimies laittaa asianomaisille henkilöille kutsun kuulemistilaisuuteen. Kuulemistilaisuuteen osallistuvat väärinkäytösepäilyn kohteena oleva käyttäjä/käyttäjät, esimies ja tietosuojavastaava sekä mahdollisuuksien mukaan henkilöstöjohtaja, organisaation lakimies ja tarvittaessa luottamusmies. Kuulemistilaisuudesta tehdään molempien osapuolten (työnantaja/työntekijä) allekirjoittama pöytäkirja, joka säilytetään hyvinvointialueen arkistonmuodostussuunnitelman mukaisesti.

6.5 Asiasta päättäminen

Kuulemistilaisuuden jälkeen työnantaja päättää, onko henkilötietojen käyttö ollut säännösten mukaista. Vakavasta rikosepäilystä tehdään aina tutkintapyyntö poliisille. Tietoturva- ja tietosuojarikosten/-rikkomusten seuraamustaulukko on tietosuojapolitiikan liite 3.

Jos kuulemistilaisuudessa todetaan, että työntekijä on syyllistynyt EU:n tietosuoja-asetuksen, kansallisten säädösten ja/tai organisaation tietosuojaohjeistusten rikkomiseen, siitä seuraa kirjallinen huomautus, varoitus tai palvelussuhteen päättämistoimien aloittaminen. Kirjallisen huomautuksen tai varoituksen antaa työntekijän esimies, eikä työntekijällä ole oikeutta hakea niihin muutosta.

Esimiehen esimiehellä on toimivalta päättää työntekijän palvelussuhteen päättämisestä. Palvelussuhteen päättämistä koskeva päätös on tehtävä kirjallisesti ja perusteltava ilmoittamalla ne seikat ja selvitykset, jotka ovat vaikuttaneet asian ratkaisuun.

6.6 Vastauksen antaminen asiakkaille tai muille viranomaisille

Henkilötietojen käytön lainmukaisuudesta selvityspyynnön tehneelle taholle lähetetään aina kirjallinen vastaus.

Jos asiakkaan tietojen käsittely on ollut perusteltua, asiakkaalle tai viranomaiselle vastataan kirjallisesti ja prosessi organisaatiossa päättyy tähän. Myös ilmenneistä väärinkäytöksistä ilmoitetaan aina kirjallisesti viranomaisille sekä asiakkaalle.

7 Raportit

Käyttölokien valvonnasta syntyy erilaisia raportteja ja selvityksiä. Tietosuojavastaava raportoi tietotilinpäätöksellä hyvinvointialueen johdolle edeltävänä vuonna suoritetusta henkilötietojen käytön valvonnasta sekä mahdollisesti havaituista epäkohdista ja puutteista tietosuojassa. Tietosuojavastaava toimii myös yhteyshenkilönä valvontaviranomaisiin raportointitehtävissä ja tietosuojan väärinkäytösepäilyissä.

Tietoturvavastaava vastaa hyvinvointialueen tietoturvasta ja sen raportoinnista.

Lokiseurantaan liittyvät asiakirjat säilytetään 12 vuotta. Raporttien ja selvitysten säilyttämisestä vastaa tietosuojavastaava.

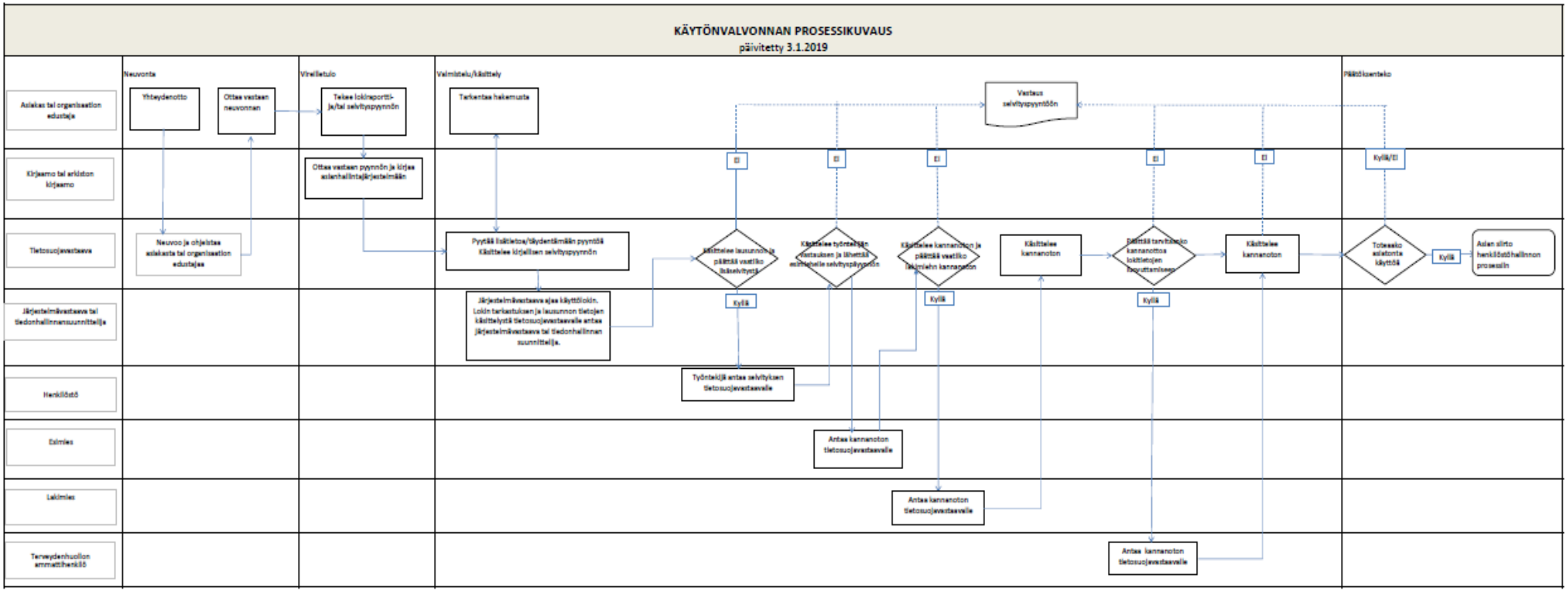
Liitteet

Liite 1 Käytönvalvonnan prosessi

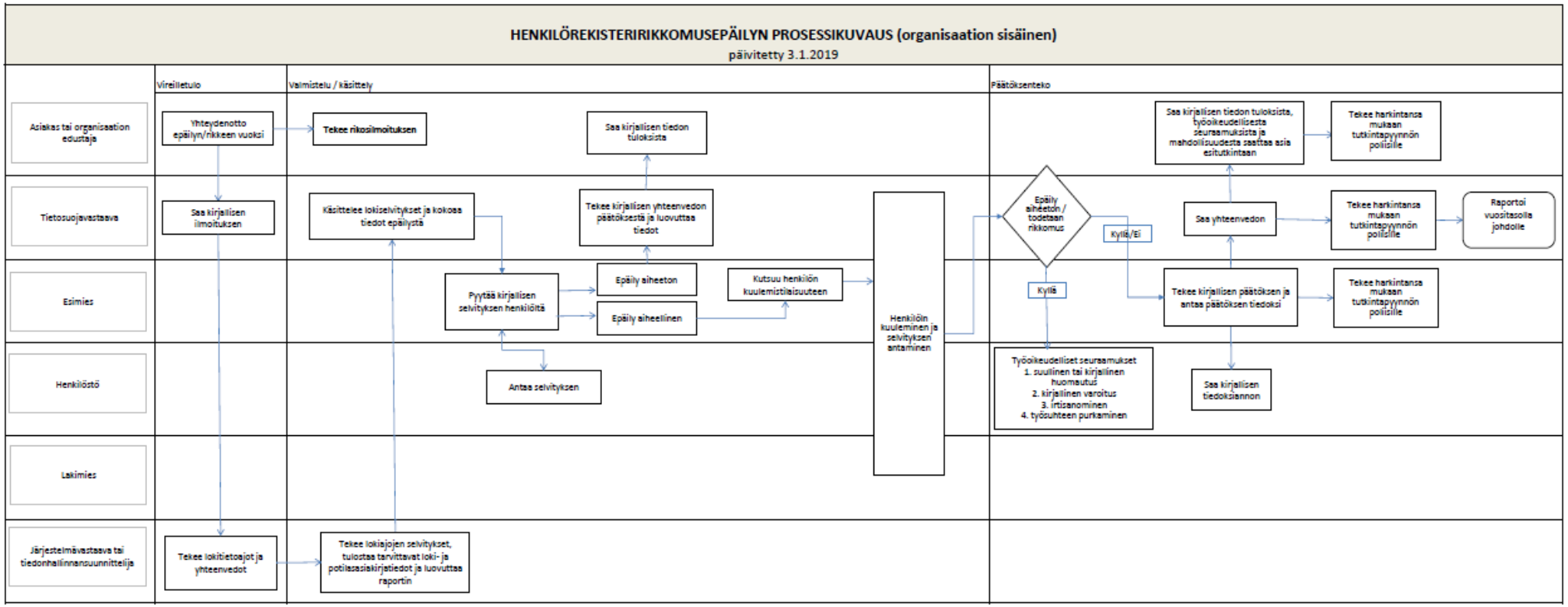
Liite 2 Henkilörekisteririkkomusepäilyn prosessi

Liite 3 Tietoturva- tietossuojarikkomusten seuraamustaulukko

Käyttölokien seuranta- ja valvontasuunnitelman liite 1



Käyttölokien seuranta- ja valvontasuunnitelman liite 2



Teon tahallisuuden aste

Rikkomuksen vakavuus

	Tietämättömyys, osaamattomuus, huolimattomuus, vahinko, tahattomuus	Piittaamattomuus, törkeä huolimattomuus, välinpitämättömyys, tahallisuus, toistuvuus	Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, salassapitorikos, aseman väärinkäyttö), hyötymistarkoitus
Lievä rikkomus (asiaton toiminta tai väärinkäyttö) **Henkilökohtaisen tietoturvan laiminlyönti Epäasiallinen käytös, haitan aiheuttaminen, resurssien tuhlaus, kulunvalvontasääntöjen rikkominen**	**Huomautus** **Opastus** **Puheeksi ottaminen**	**Kirjallinen varoitus** **Opastus** **Huomautus** **Puheeksi ottaminen**	**Tutkintapyyntöä poliisille harkitaan** **Kirjallinen varoitus**
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen **Ohjelmien ja pelien luvaton kopiointi, luvattomien ohjelmien asentaminen, ylläpitäjän työkalujen luvaton hallussapito, palvelun luvaton pystytys, tunnuksen luovuttaminen, tiedon luottamuksellisuuden vaarantaminen**	**Kirjallinen varoitus** **Huomautus**	**Työnantaja käynnistää palvelussuhteen päättämismenettelyn** **Käyttöoikeuden peruminen** **Kirjallinen varoitus**	**Työnantaja käynnistää palvelussuhteen päättämismenettelyn** **Tutkintapyyntö poliisille** **Kirjallinen varoitus**
Vakava rikkomus/rikos **Potilas/asiakastiedon tai liikesalaisuuden luvaton käsittely ja luovuttaminen, hakkerointi, tunkeutuminen, rikoslain alaisen materiaalin oikeudeton käsittely, virusten tahallinen levittäminen**	**Työnantaja käynnistää palvelussuhteen päättämismenettelyn** **Tutkintapyyntöä poliisille harkitaan** **Kirjallinen varoitus**	**Työnantaja käynnistää palvelussuhteen päättämismenettelyn** **Tutkintapyyntö poliisille** **Kirjallinen varoitus**	**Työnantaja käynnistää palvelussuhteen päättämismenettelyn** **Tutkintapyyntö poliisille**

Lievä rikkomus (asiaton toiminta tai väärinkäyttö)

- henkilökohtaisen tietoturvan/tietosuojan laiminlyönti (käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin)
- haitan aiheuttaminen (laitteiden/ohjelmien lukitseminen ja toisen oikeutetun pääsyn estäminen)
- resurssien tuhlaus (työajan väärinkäyttö, asiaton surffailu internetissä)
- luvaton kaupallinen tai poliittinen toiminta (sähköpostin käyttäminen henkilökohtaiseen markkinointiin)
- kulunvalvontaohjeiden rikkominen (esim. avainten luovuttaminen toisen käyttöön)

Rikkomus (vakava väärinkäyttö tai turvallisuuden rikkominen)

- ohjeiden vastainen laitteistojen tai ohjelmien käyttö
- käyttäjätunnuksen luovuttaminen (salasanan luovuttaminen toiselle käyttäjälle tai avoimen työaseman luovuttaminen niin, että toinen henkilö pääsee valvomatta käyttämään luovuttajan tunnusta)
- tiedon luottamuksellisuuden vaarantaminen (työaseman jättäminen auki valvomatta tai asiakas/potilastiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä)
- ylläpito-oikeuksien luvaton hallussapito
- ohjelmien, pelien luvaton kopiointi
- luvattomien ohjelmien asentaminen
- luvattomien laitteiden lisääminen verkkoon

Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)

- salassa pidettävien tietojen oikeudeton käsittely/ luovuttaminen (esim. potilas/ asiakastietojen katsominen ilman oikeudellista perustetta)
- tietojen luvaton käyttö (esim. tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely ja hallussapito mm. rasistinen aineisto tai lapsiporno)
- hakkerointi ja tunkeutuminen tietojärjestelmiin
- vakoilu
- virka-aseman väärinkäyttö
- hyötymistarkoitus