Kela / Kanta-palvelut

1.11.2021

Liite Kanta-palvelujen asiakkuuden sitoumukseen: Kuvaus Kanta-palveluihin liittyvien palvelujen yhteisrekisterinpitäjyydestä

1. Asiakirjan tarkoitus ja osapuolet, joita se koskee

Tämän Kanta-palvelujen asiakkuuden sitoumuksen liiteasiakirjan tarkoituksena on kuvata sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (784/2021, jäljempänä asiakastietolaki) 4 §:n 3 momentin sekä sähköisestä lääkemääräyksestä annetun lain (61/2007, jäljempänä reseptilaki) 18 §:n mukaisten yhteisrekisterinpitäjyyksien vastuualueet. Tähän liittyen tässä asiakirjassa määritellään yhteisrekisterinpitäjyyteen liittyvät menettelytavat rekisteröidyn oikeuksien sekä muiden rekisterinpitäjille kuuluvien velvollisuuksien toteuttamiseksi. Tällä asiakirjalla tai muilla rekisterinpitäjien keskinäisillä järjestelyillä ei voida määritellä tai sopia rekisterinpitäjien vastuista asiakastietolaissa tai muussa lainsäädännössä määritellystä poikkeavasti.

Tämä liiteasiakirja koskee sosiaali- ja terveydenhuollon luovutuslokitietojen, tahdonilmaisupalvelun, tiedonhallintapalvelun osalta yhteisrekisterinpitäjiä, joita ovat Kansaneläkelaitos (jäljempänä Kela) sekä sosiaali- ja terveydenhuollon palvelunantajat. Reseptikeskuksen osalta tämä asia koskee yhteisrekisterinpitäjiä, joita ovat Kela, apteekit sekä sosiaali- ja terveydenhuollon palvelunantajat ja itsenäiset lääkkeen määrääjät, jotka laativat sähköisiä lääkemääräyksiä.

EU:n yleisen tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, jäljempänä tietosuoja-asetus) 26 artiklan ensimmäisen kohdan mukaan, jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Ne määrittelevät keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueen tässä asetuksessa vahvistettujen velvoitteiden noudattamiseksi, erityisesti rekisteröityjen oikeuksien käytön ja 13 ja 14 artiklan mukaisten tietojen toimittamista koskevien tehtäviensä osalta, paitsi jos ja siltä osin kuin rekisterinpitäjiin sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä määritellään rekisterinpitäjien vastuualueet. Saman artiklan toisen kohdan mukaan 1 kohdassa tarkoitetusta järjestelystä on käytävä asianmukaisesti ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla.

Tietosuoja-asetuksen 26 artiklan kolmannen kohdan mukaan riippumatta tarkoitetun järjestelyn ehdoista rekisteröity voi käyttää tämän asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.

Asiakastietolain 4 §:n 3 momentin mukaan kukin sosiaali- ja terveydenhuollon palvelunantaja ja Kela ovat sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien ja tiedonhallintapalvelun sekä tahdonilmaisupalvelun yhteisrekisterinpitäjiä.

- Kela vastaa yhteisrekisterinpitäjänä tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja hävittämisestä siten kuin asiakastietolain 14 §:ssä säädetään.
- Tiedonhallintapalveluun koostettavia tietoja tallentavat ja tahdonilmaisupalveluun tietoja tallentavat palvelunantajat vastaavat tallennettavien tietojen oikeellisuudesta sekä muista rekisterinpitäjän velvoitteista.
- Kela toimii tietosuoja-asetuksen 26 artiklan 1 kohdan mukaisena rekisteröidyn yhteyspisteenä.

Asiakastietolain 4 §:n 5 momentin mukaan reseptikeskuksen rekisterinpitäjästä säädetään reseptilain 18 §:ssä. Reseptilain uuden 18 §:n 1 momentin (786/2021) mukaan reseptikeskus on Kelan, apteekkien ja sähköisiä lääkemääräyksiä laativien palvelunantajien ja itsenäisten lääkkeen määrääjien yhteisrekisteri. Reseptilain 18 §:n 2–4 momenttien mukaan:

- Kela vastaa reseptikeskuksessa olevien tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja hävittämisestä.
- Sähköisiä lääkemääräyksiä laativa palvelunantaja ja itsenäinen lääkkeen määrääjä vastaavat Reseptikeskukseen tallennettavan lääkemääräyksen tietojen oikeellisuudesta.
- Lääkkeen toimittanut apteekki vastaa reseptikeskukseen tallennettavien toimitustietojen oikeellisuudesta.
- Kela vastaa tietosuoja-asetuksessa rekisterinpitäjälle säädetyistä muista kuin tässä laissa apteekeille ja sähköisiä lääkemääräyksiä laativille palvelunantajille ja itsenäisille lääkkeen määrääjille asetetuista velvoitteista.
- Kela toimii lisäksi tietosuoja-asetuksen 26 artiklan 1 kohdan mukaisena rekisteröidyn yhteyspisteenä.

2. Määritelmät

Tässä asiakirjassa tietosuojalainsäädännöllä tarkoitetaan tietosuoja-asetusta mahdollisine muutoksineen, tietosuojalakia (1050/2018) sekä tietosuojaviranomaisten tai tuomioistuinten henkilötietojen käsittelyä koskevia päätöksiä, ohjeita ja neuvonantoja. Ellei toisin mainita, henkilötiedolla, henkilötiedon käsittelyllä, henkilötietojen käsittelijällä, rekisterinpitäjällä, yhteisrekisterinpitäjällä, rekisteröidyllä, henkilörekisterillä, tietosuojaviranomaisella ja henkilötietojen tietoturvaloukkauksella on tietosuoja-asetuksen mukainen määritelmä.

Sosiaali- ja terveydenhuollon palvelunantajalla tarkoitetaan tässä asiakirjassa palvelunantajaa, joka on liittynyt Kanta-palvelujen käyttäjäksi ja näin ollen käyttää arkistointipalvelua, tiedonhallintapalvelua sekä tahdonilmaisupalvelua tai reseptikeskusta. Sosiaali- ja terveydenhuollon palvelunantajia ovat myös rekisterinpitovastuulliset itsenäiset ammatinharjoittajat, jotka toiminnassaan esimerkiksi käyttävät tiedonhallinta- sekä tahdonilmaisupalveluita ja toimivat näin kyseisten palvelujen yhteisrekisterinpitäjänä. Itsenäiset ammatinharjoittajat toimivat myös reseptikeskuksen yhteisrekisterinpitäjänä, mikäli he toiminnassaan laativat ja tallentavat sähköisiä lääkemääräyksiä reseptikeskukseen.

3. Palvelujen kuvaukset ja niissä käsiteltävät henkilötiedot

3.1 Tiedonhallintapalvelu

Tiedonhallintapalvelu on osa asiakastietolain 6 §:n mukaisia valtakunnallisia tietojärjestelmäpalveluja. Tiedonhallintapalvelu koostaa potilasasiakirjoista terveydenhuollon toteuttamisen kannalta keskeiset potilastiedot ja tuottaa niistä yhteenvetoja palvelunantajalle potilaan hoidon toteuttamista varten. Keskeisiä potilastietoja, jotka tiedonhallintapalvelu voi koostaa, ovat diagnoosit ja käyntisyyt, riskit, laboratoriotulokset, rokotukset, toimenpiteet, lääkitystiedot, fysiologiset mittaukset ja toimenpidekoodistolla kirjatut kuvantamistutkimukset, toimintakykyyn liittyvät tiedot, ajanvaraustiedot. Lisäksi tiedonhallintapalveluun tallennetaan ylläpidettävät asiakirjat, kuten potilaslain 4 a §:n mukainen suunnitelma potilaan tutkimuksesta, hoidosta tai kuntoutuksesta tai muu vastaava suunnitelma.

3.2 Tahdonilmaisupalvelu

Tahdonilmaisupalvelu on osa asiakastietolain 6 §:n mukaisia valtakunnallisia tietojärjestelmäpalveluja. Asiakastietolain 12 §:n mukaisesti tahdonilmaisupalveluun on tallennettava tieto henkilölle annetusta tämän lain ja sähköisestä lääkemääräyksestä

annetun lain mukaisista informoinneista sekä henkilön antamista asiakastietojen luovutusta koskevista luovutusluvista, suostumuksista ja kielloista. Lisäksi tahdonilmaisupalveluun voidaan tallentaa myös tieto muista kuin mainituista henkilön terveyden- ja sairaanhoitoon tai sosiaalipalveluihin liittyvistä tahdonilmauksista sekä muista henkilön sosiaali- ja terveysalan palveluihin ja asiakastietojen käsittelyyn liittyvistä tahdonilmauksista.

3.3 Sosiaali- ja terveydenhuollon luovutuslokit

Palvelunantajan on kerättävä lokitiedot asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja luovutuksesta seurantaa ja valvontaa varten (asiakastietolain 25 §). Sosiaali- ja terveydenhuollon luovutuslokilla tarkoitetaan lokia, joka sisältää tiedot henkilötietojen luovutuksesta eri rekisterien tai rekisterinpitäjien välillä. Luovutuslokirekisteriin tallennetaan tieto luovutetuista asiakastiedoista, siitä palvelunantajasta, jonka asiakastietoja luovutetaan, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta sekä luovutusajankohdasta.

3.4 Reseptikeskus

Reseptikeskus on tietokanta, joka koostuu lääkkeen määrääjien tallentamista sähköisistä lääkemääräyksistä, apteekkien reseptilain 12 §:ssä säädetyillä perusteilla tallentamista lääkemääräyksistä, sosiaali- ja terveydenhuollon palvelunantajien reseptilain 23 §:ssä säädetyillä perusteilla potilaille luovutettuja lääkkeitä koskevista tiedoista, lääkemääräyksiin liitetyistä toimitustiedoista ja lääkehoidon arviointiin liittyvistä merkinnöistä (reseptilain 3 §:n 1 momentin 4 kohta).

4. Henkilötietojen käsittelyperusta ja oikeus henkilötietojen käsittelyyn

Sosiaali- ja terveydenhuollon palveluantajat voivat tallentaa tahdonilmaisupalveluun sekä tiedonhallintapalveluun tietoja vain potilaan hoidon tai palvelun toteuttamista varten. Palvelunantajat voivat käsitellä tallennettuja tietoja vain palvelun tai hoidon toteuttamista varten, ellei asiakas ole kieltänyt tietojensa luovuttamista. Asiakkaan antamista luovutusluvasta, suostumuksesta ja kielloista on säädetty muun ohella asiakastietolain 18 §:ssä. Potilas- ja asiakastietojen luovuttamisesta valtakunnallisten tietojärjestelmäpalvelujen välityksellä säädetty muun ohella asiakastietolain 20 ja 21 §:ssä sekä reseptilain 13 §:ssä.

Reseptikeskuksen osalta apteekit voivat käsitellä reseptikeskuksen tietoja lääkemääräyksen toimittamista ja tähän liittyviä tehtäviä varten. Apteekkien tiedonsaantioikeudesta on säädetty

reseptilain 11 §:ssä. Sosiaali- ja terveydenhuollon palvelunantaja sekä itsenäiset ammatinharjoittajat voivat käsitellä reseptikeskuksen tietoja potilaan hoidon ja lääkityksen seurantaa ja toteuttamista varten. Reseptikeskuksen tietojen luovuttamisesta ja kielto-oikeudesta on säädetty reseptilain 13 §:ssä.

Tässä asiakirjassa tarkoitettujen yhteisrekistereihin tallennettujen henkilötietojen käsittelyperusta on lainsäädäntö. Käyttöoikeudesta asiakastietoon on säädetty asiakastietolain 15 §:ssä sekä sen nojalla annettavassa asetuksessa ja sähköisten lääkemääräystietojen osalta reseptilain 4 luvussa. Tässä asiakirjassa tarkoitettuihin palveluihin tallennettuja henkilötietoja ei siirretä EU:n/ETA:n ulkopuolelle. Lisäksi Pilvipalveluiden turvallisuuden arviointikriteerit edellyttävät[1], että yhteiskunnan kannalta kriittisen toiminnan kannalta olennaisen tietojärjestelmän on oltava Suomessa. Lisäksi arkaluontoisesten henkilötietojen keskittymän on oltava Suomessa. Mikäli apteekki- tai potilastietojärjestelmä tarjotaan pilvipalveluna, edellä mainitut PiTuKri:n vaatimukset on otettava huomioon.

5. Yhteisrekisterinpitäjien vastuut

5.1 Yleistä yhteisrekisterinpitäjien vastuista ja velvollisuuksista

Tässä asiakirjassa tarkoitetut yhteisrekisterinpitäjät toimivat tietosuoja-asetuksen tarkoittamana rekisteripitäjänä ja vastaavat näin itsenäisesti suorittamiensa henkilötietojen käsittelytoimien oikeellisuudesta asiakastietolaissa sekä reseptilaissa säädetyin vastuin. Yhteisrekisterinpitäjät vastaavat suorittamiensa henkilötietojen käsittelytoimien oikeellisuudesta voimassa olevan tietosuojalainsäädännön mukaisesti. Tässä asiakirjassa yhteisrekisterinpitäjiä ovat edellä mainitun mukaisesti:

- Tiedonhallintapalvelu: sosiaali- ja terveydenhuollon palvelunantajat sekä Kela.
- Tahdonilmaisupalvelu: sosiaali- ja terveydenhuollon palvelunantajat sekä Kela.
- Sosiaali- ja terveydenhuollossa syntyneet luovutuslokit: sosiaali- ja terveydenhuollon palvelunantajat sekä Kela.
- Reseptikeskus: sosiaali- ja terveydenhuollon palvelunantajat, itsenäiset lääkkeen määrääjät, apteekit sekä Kela.

[1] Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Yhteisrekisterinpitäjyyden kannalta on huomioitava, että rekisteröidyllä on oikeus käyttää tietosuoja-asetuksen oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.

5.2 Rekisteröityjen informointi ja rekisteröidyn oikeuksien käyttäminen

Kela toimii asiakastietolain sekä reseptilain mukaan tiedonhallintapalvelun, tahdonilmaisupalvelun, sosiaali- ja terveydenhuollon luovutuslokien sekä reseptikeskuksen tietosuoja-asetuksen 26 artiklan mukaisena yhteyspisteenä suhteessa rekisteröityihin. Kela vastaa yhteyspisteenä tietosuojalainsäädännössä rekisterinpitäjille asetetun informointivelvoitteen täyttämisestä ja toteuttamisesta tässä asiakirjassa mainittuihin palveluihin kerättyjen henkilötietojen osalta. Tarvittaessa yhteisrekisterinpitäjien tulee yhteistyössä avustaa ja vastata tietosuoja-asetuksen mukaisen rekisteröidyn informointivelvoitteen toteuttamisessa siltä osin kuin se kuuluu kyseessä olevalle yhteisrekisterinpitäjälle.

Kela toimii ensisijaisena yhteyspisteenä rekisteröityjen oikeuksien käyttämistä koskevissa pyynnöissä. Kelan roolista yhteyspisteenä ilmoitetaan rekisteröidyille edellä tarkoitetussa rekisteröidylle toimitettavassa informaatiossa. Mikäli rekisteröidyn yhteydenotto koskee palvelunantajan, itsenäisen ammatinharjoittajan tai apteekin vastuulla olevaa asiaa, kuten tietojen oikeellisuutta, Kela osoittaa asiakkaan yhteydenoton sille palvelunantajalle, jota kyseinen yhteydenottopyyntö koskee ja joka on kyseisen kirjauksen kyseessä olevaan palveluun tehnyt tai jonka tehtäviin asia muutoin sisältyy.

Muilta osin rekisteröidyn oikeudet tulee kuvata yhteisrekisterinpitäjien omissa tietosuojaselosteissa. Myös tämän asiakirjan keskeinen sisältö tulee ilmetä selkeästi ja läpinäkyvästi kyseessä olevaa palvelua koskevista tietosuojaselosteista. Palvelunantajat, apteekit sekä itsenäiset ammatinharjoittavat laativat tahollaan tietosuoja-asetuksen 30 artiklan mukaisen selosteen vastuullaan olevista henkilötietojen käsittelytoimista. Mainitut tahot osaltaan huolehtivat siitä, että seloste ja siinä olevat yhteystiedot ovat ajantasaisia ja että sitä päivitetään tarvittaessa. Kela laatii oman selosteen vastuullaan olevista henkilötietojen käsittelytoimista kyseessä olevien valtakunnallisten tietojärjestelmäpalvelujen osalta.

5.3 Rekisteröidyn tarkastuspyyntö

5.3.1 Tiedonhallintapalvelu

Rekisteröidyllä on oikeus tarkastaa hänestä tiedonhallintapalveluun tallennetut tiedot. Palvelunantaja on toiminnassaan syntyneiden tietojen rekisterinpitäjä ja se vastaa yhteisrekisterinpitäjänä tiedonhallintapalveluun koostettavien tietojen oikeellisuudesta. Mikäli rekisteröity käyttää tarkastusoikeuttaan, osoitetaan sekä tarvittaessa ohjataan tätä koskeva pyyntö sille palvelunantajalle, joka vastaa kirjatun tiedon oikeellisuudesta sekä muista rekisterinpitäjän velvollisuuksista. Palvelunantajan tulee toimittaa rekisteröidylle hänestä tallennetut tiedot tietosuoja-asetuksen mukaisesti. Rekisteröidyn on mahdollista katsella tiedonhallintapalveluun tallennettuja tietoja koostetusti Omakanta-palvelun kautta.

5.3.2 Tahdonilmaisupalvelu

Rekisteröidyllä on oikeus tarkastaa hänestä tahdonilmaisupalveluun tallennetut tiedot. Siltä osin kuin palvelunantaja tai itsenäinen ammatinharjoittaja on kirjannut tahdonilmaisupalveluun tietoja, se vastaa yhteisrekisterinpitäjänä tahdonilmaisupalveluun tallentamiensa tietojen oikeellisuudesta. Mikäli rekisteröity käyttää tarkastusoikeuttaan, osoitetaan sekä tarvittaessa ohjataan tätä koskeva pyyntö sille palvelunantajalle, joka on kyseessä olevan kirjauksen tahdonilmaisupalveluun tehnyt ja joka vastaa kirjaamansa tiedon oikeellisuudesta ja muista rekisterinpitäjälle kuuluvista velvollisuuksista. Palvelunantajan tulee toimittaa rekisteröidylle hänestä tallennetut tiedot tietosuoja-asetuksen mukaisesti.

Rekisteröidyn on mahdollista katsella antamiaan tahdonilmaisuja kootusti Omakanta-palvelun kautta. Tarvittaessa Kela voi toimittaa rekisteröidylle hänen itsensä tahdonilmaisupalveluun tallentamat tiedot. Mikäli rekisteröidyn ei ole mahdollista saada tahdonilmaisupalveluun tallennettuja tietoja kootusti palvelunantajilta, Kela voi rekisteröidyn yhteyspisteenä tarvittaessa luovuttaa rekisteröidylle nämä tiedot. Näissä tilanteissa Kela toimittaa rekisteröidylle hänestä tallennetut tiedot tietosuoja-asetuksen mukaisesti.

5.3.3 Reseptikeskus

Rekisteröidyllä on oikeus tarkastaa hänestä reseptikeskukseen tallennetut tiedot. Reseptikeskuksen osalta potilaan tiedonsaantioikeudesta ja tietojen korjaamisesta on säädetty reseptilain 16 §:ssä. Reseptikeskuksessa olevien virheellisten tietojen oikaisemisesta säädetään reseptilain 10 §:ssä ja tietosuoja-asetuksen 16 artiklassa. Jos

potilas tai hänen laillinen edustajansa vaatii tiedon oikaisua tietosuoja-asetuksen 16 artiklan perusteella ja virheellinen tieto perustuu lääkkeen määrääjän tai lääkkeen toimittajan tekemään merkintään, vaatimus oikaisemisesta on osoitettava virheellisen merkinnän tehneelle henkilölle tai sille organisaatiolle, jonka palveluksessa virheen tehnyt henkilö on ollut virheen tehdessään.

Siltä osin kuin rekisteröidyn tarkastuspyyntö koskee reseptikeskukseen tallennettuja tietoja, vastaa Kela tarkastuspyynnön toteuttamisesta ja siitä, että rekisteröidylle kuuluva oikeus saada pääsy tietoihin toteutuu, sillä Kela vastaa pykälän mukaisesti muista rekisterinpitäjälle kuuluvista velvollisuuksista. Kela toimittaa rekisteröidylle hänestä tallennetut tiedot tietosuoja-asetuksen mukaisesti.

Mikäli rekisteröity haluaa korjata hänestä reseptikeskukseen tallennettuja tietoja, osoitetaan tätä koskeva pyyntö vastuussa olevalle palvelunantajalle reseptilain 16 §:n mukaisesti.

5.3.4 Sosiaali- ja terveydenhuollossa syntyneet luovutuslokitiedot sekä muut luovutuslokitiedot

Asiakastietolain 4 § mukaan Kela ja palveluantaja ovat sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien yhteisrekisterinpitäjiä. Kela vastaa yhteisrekisterinpitäjänä tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja hävittämisestä siten kuin 14 §:ssä säädetään. Tältä osin palvelunantajan, jonka toiminnassa luovutuslokimerkintä on syntynyt, vastaa tallentuneen tiedon oikeellisuudesta sekä siihen liittyvistä tarkastuspyynnöistä.

Asiakastietolain 26 §:n 1 momentin mukaan asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten palvelunantajalta kirjallisesta pyynnöstä kohtuullisessa ajassa ja viimeistään kahden kuukauden kuluessa lokirekisterin perusteella maksutta tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste. Saman lainkohdan mukaan asiakkaalla on vastaava oikeus saada Kelalta muun ohella tiedonhallintapalvelun, tahdonilmaisupalvelun, reseptikeskuksen lokitiedot, käytettyjen tai luovutettujen asiakastietojen lokitiedot sekä tiedot käyttö- ja luovutusajankohdasta siltä osin kuin tiedot kuuluvat Kelan rekisterinpitoon.

Reseptilain 16 §:n 3 momentin mukaan potilaalla on oikeus pyynnöstä saada lokitietojen perusteella tieto siitä, ketkä ovat käsitelleet ja katselleet häntä koskevia reseptikeskuksessa

tai asiakastietolain 12 §:ssä tarkoitetussa tahdonilmaisupalvelussa olevia tietoja. Potilaalla ei kuitenkaan ole oikeutta saada lokitietoja, jos lokitietojen luovuttajan tiedossa on, että lokitietojen antamisesta saattaisi aiheutua vakavaa vaaraa potilaan terveydelle tai hoidolle taikka jonkun muun oikeuksille. Myöskään kahta vuotta vanhempia lokitietoja ei ole oikeutta saada, ellei siihen ole erityistä syytä. Potilas ei saa käyttää tai luovuttaa saamiaan lokitietoja edelleen muuhun käyttötarkoitukseen. Kelan on annettava tiedot viivytyksettä. Tietojen antamisesta ei saa periä maksua. Jos potilas pyytää uudelleen tietoja, jotka hän on jo saanut, hänellä on oikeus saada tiedot vain, jos siihen on perusteltu syy hänen etujensa tai oikeuksiensa toteuttamiseksi. Asia voidaan saattaa tietosuojavaltuutetun käsiteltäväksi tietosuojalain 21 §:n 1 momentin mukaisesti. Kansaneläkelaitos saa periä uudelleen annettavista tiedoista maksun, joka ei saa ylittää tietojen antamisesta aiheutuvia kustannuksia. (Ks.asiakastietolain 26 § ja reseptilain 16 §).

Mikäli rekisteröidyn tarkastuspyyntö koskee tiedonhallintapalvelun, tahdonilmaisupalvelun tai reseptikeskuksen luovutuslokitietoja tai reseptikeskuksen käyttölokitietoja, kuuluu tämän pyynnön toteuttaminen ja siihen vastaaminen Kelalle. Mikäli rekisteröidyn tarkastuspyyntö kohdistuu sosiaali- ja terveydenhuollon palvelunantajan toiminnassa syntyneisiin käyttölokitietoihin, kuuluu tämän asian toteuttaminen sille palvelunantajalle, jonka toiminnassa kyseinen käyttömerkintä on syntynyt (asiakastietolain 4 §). Lisäksi asiakastietolain 24 §:n 2 momentin mukaisesti rekisteröidylle saadaan näyttää Omakanta-palvelun välityksellä hänen tietojensa käsittelyä koskevat luovutus- ja käyttölokitiedot lukuun ottamatta luovutuksensaajan henkilötietoja.

5.4 Rekisteröidyn korjauspyyntö ja tietojen poistaminen

Palveluun tallennetun tiedon oikeellisuudesta vastaavan palvelunantajan vastuulla on tiedonhallintapalveluun, reseptikeskukseen sekä tahdonilmaisupalveluun tallennettujen tietojen oikaisemiseen ja poistamiseen liittyvän menettelyn toteuttaminen tietosuoja-asetuksen 16 ja 17 artiklan mukaisesti. Rekisteröidyn ollessa yhteydessä Kelaan, Kela vastaa rekisteröidyn yhteyspisteenä siitä, että palvelunantaja saa rekisteröidyn yhteydenoton käsiteltäväkseen.

Rekisteröidyllä on oikeus pyytää tietojensa poistamista, mutta potilas- ja asiakasasiakirjojen sekä reseptitietojen säilyttämistä koskeva sääntely rajoittaa tämän oikeuden toteuttamista. Potilas- ja asiakasasiakirjojen sekä lääkemääräysasiakirjojen sekä näiden lokitietojen säilyttämisajoista on säännelty muun ohella asiakastietolaissa, potilaslaissa (785/1992), potilasasiakirja-asetuksessa (298/2009), sosiaalihuollon asiakasasiakirjalaissa (254/2015) sekä reseptilaissa. Silloin, kun säilytysajat perustuvat pakottavaan lainsäädäntöön, ei

rekisteröidyllä ole oikeutta saada häntä koskevia asiakirjoja tai niiden sisältämiä tietoja taikka näitä koskevia lokitietojaan poistetuksi ennen laissa säädetyn säilytysajan päättymistä.

6. Tietoturvaloukkauksissa- ja poikkeamissa noudatettavat menettelyt

6.1 Yleistä yhteisrekisterinpitäjien vastuista tietoturvaloukkaustilanteissa

Kaikki yhteisrekisterinpitäjät dokumentoivat havaitsemansa mahdolliset henkilötietojen tietoturvaloukkaukset- ja poikkeamat itsenäisesti ja vastaavat omalta osaltaan tietosuoja-asetuksen 33 ja 34 artiklan mukaisten ilmoitusten tekemisestä, mikäli loukkaus on sellainen, että se tätä edellyttää. Ilmoitusvelvollisuus koskee sekä valvontaviranomaiselle tehtävää ilmoitusta että rekisteröidyn informointia tilanteessa, jossa tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Ilmoitusvelvollisuuden toteuttamiseen liittyvistä määräajoista on säädetty tietosuoja-asetuksessa.

Jokainen yhteisrekisterinpitäjä on vastuussa oman toimintansa varautumisesta mahdollisiin tietoturvaloukkauksiin ja niiden asianmukaiseen käsittelyyn. Yhteisrekisterinpitäjät vastaavat omassa toiminnassaan siitä, että sen palveluksessa toimivalla henkilöstöllä on ohjeet siitä, kehen tai mihin heidän tulee olla yhteydessä mahdollisessa tietoturvaloukkaustilanteessa. Jokainen yhteisrekisterinpitäjä on omassa toiminnassaan vastuussa omista tietoturvaloukkausprosesseistaan, -ohjeistaan, sekä tarvittavasta vastuunjaosta kyseessä olevan toiminnan kannalta.

Asiakastietolain 41 §:ssä on säädetty ilmoittamisvelvollisuudesta tietojärjestelmän olennaisten vaatimusten poikkeamista. Mikäli tietoturvaloukkaus johtuu Kanta-palvelujen, apteekkijärjestelmän, asiakas- tai potilastietojärjestelmän toiminnasta, on oletettavaa, että järjestelmä ei täytä asiakastietolain sille asetettuja tietoturvavaatimuksia ja kyseessä on poikkeus olennaisissa vaatimuksissa. Kyseessä olevassa tilanteessa tietojärjestelmän valmistajalla sekä järjestelmää käyttävällä palvelunantajalla ja apteekilla on asiakastietolain 41 §:n mukaisesti velvollisuus ilmoittaa asiasta Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Muun ohella myös Kelalla on kyseinen ilmoitusvelvollisuus asiakastietolain 41 §:n mukaisesti.

Yhteisrekisterinpitäjät vastaavat siitä, että ne kykenevät omassa toiminnassaan havaitsemaan mahdolliset tietoturvaloukkaustilanteet riittävän nopeasti sekä siitä, että tähän liittyvä havainnointi on sisällytetty yhteisrekisterinpitäjän omiin prosesseihin.

6.2 Vastuunjako eri palveluissa

Tiedonhallintapalvelun ja tahdonilmaisupalvelun osalta palvelunantajat vastaavat asiakastietolain 4 §:n mukaisesti muista rekisterinpitäjälle kuuluvista velvoitteista. Näin ollen johtava vastuu näiden palveluiden henkilötietojen tietoturvaloukkausten ilmoittamisesta on kyseessä olevalla palvelunantajalla. Sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien osalta Kela vastaa yhteisrekisterinpitäjänä tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja hävittämisestä asiakastietolain 14 § mukaisesti. Näiltä osin Kela vastaa myös palvelussa ilmenevistä mahdollisista tietoturvaloukkauksista.

Reseptikeskuksen osalta Kela vastaa reseptilain 18 §:n mukaan tietosuoja-asetuksessa rekisterinpitäjälle säädetyistä muista kuin tässä laissa apteekeille ja sähköisiä lääkemääräyksiä laativille palvelunantajille ja itsenäisille lääkkeen määrääjille asetetuista velvoitteista. Näin ollen johtava vastuu reseptikeskuksen henkilötietojen tietoturvaloukkausten ilmoittamisesta on Kelalla. Mikäli reseptikeskuksen tietoturvaloukkaus tapahtuu muun yhteisrekisterinpitäjän omassa toiminnassa, kuten reseptitietojen käsittelyssä, ensisijainen vastuu ilmoitusvelvollisuuden toteuttamisesta on sillä yhteisrekisterinpitäjällä, jonka toiminnassa epäilty loukkaus on tapahtunut.

6.3 Noudatettavat menettelytavat

6.3.1 Lähtökohta tietoturvaloukkausten ilmoittamiseen eri tilanteissa

Siitä riippumatta, mitä yhteisrekisterinpitäjien vastuusta on säädetty, ensimmäisen havainnon tietoturvaloukkauksesta voi tehdä kuka tahansa taho, joka mahdollisen tietoturvaloukkauksen ensimmäiseksi havaitsee. Havaitsijan tulee ottaa yhteys edustamansa organisaation tietoturvaloukkauksen yhteydenottotahoon, jolle ilmoittaa oman laitoksensa ohjeistuksen mukaiset tiedot.

Jos tietoturvaloukkaus kohdistuu vain yhden yhteisrekisterinpitäjän toimintaan ja kyse on siis organisaation sisäisestä loukkauksesta, loukkausjatkoselvitetään ja ratkaistaan kyseessä olevan yhteisrekisterinpitäjän sisäisen prosessin ja ohjeistusten mukaisesti. Tällöin se yhteisrekisterinpitäjä, jonka toimintaan mahdollinen tietoturvaloukkaus kohdistuu vastaa tietosuoja-asetuksen 33 ja 34 artiklojen mukaisen ilmoitusvelvollisuuden toteuttamisesta. Mikäli epäilty tietoturvaloukkaus kohdistuu tai sen arvioidaan kohdistuvan jonkin palvelun sisällä useaan palvelunantajaan, itsenäiseen ammatinharjoittajaan tai apteekkiin, mutta ei

Kelan ylläpitämiin palveluihin, tulee näiden rekisterinpitäjien yhdessä päättää ja koordinoida selvitystehtävä ja laatia mahdollinen loukkausilmoitus valvontaviranomaiselle ja tarvittaessa informoida rekisteröityä.

Mikäli palvelunantaja havaitsee mahdollisen tietoturvaloukkauksen Kelan ylläpitämässä palvelussa tai sen toiminnassa taikka Kelan vastuulle muutoin yhteisrekisterinpitäjänä kuuluvassa toiminnossa, tulee palvelunantajan olla viipymättä yhteydessä Kelaan asian selvittämiseksi. Kela vastaa näissä tilanteissa tietosuoja-asetuksen 33 ja 34 artiklojen mukaisten ilmoitusvelvollisuuksien toteuttamisesta.

Jos tietoturvaloukkaus kohdistuu tai sen arvioidaan kohdistuvan sekä Kelaan että toiseen yhteisrekisterinpitäjään tai näiden toimintaan, yhteisrekisterinpitäjien tulee ilmoittaa loukkausepäilystä viipymättä toisilleen. Kelan osalta yhteisrekisterinpitäjän tulee ilmoittaa asiasta Kelan tekniseen tukeen. Muiden yhteisrekisterinpitäjien tulee ilmoittaa tähän liittyen yhteystiedot tämän asiakirjan kohdan 8 mukaisesti. Jos näissä tilanteissa tietoturvaloukkaus kohdistuu reseptikeskukseen, vastaa tietosuoja-asetuksen 33 ja 34 artiklojen mukaisen ilmoitusvelvollisuuden toteuttamisesta Kela. Jos tietoturvaloukkaus kohdistuu tiedonhallinta- tai tahdonilmaisupalveluun, vastaa ilmoitusvelvollisuuden toteuttamisesta se palvelunantaja, joka vastaa kyseessä olevassa tilanteessa muista rekisterinpitäjälle kuuluvista velvollisuuksista.

Jos tietoturvaloukkaus tapahtuu Kelan ylläpitämässä palvelussa ja loukkaus liittyy Kelan toimintaan, tulee Kelan koordinoida ja laatia mahdollinen ilmoitus tietosuojavaltuutetun toimistolle ja tarvittaessa rekisteröidylle. Mikäli palvelunantaja havaitsee mahdollisen tietoturvaloukkauksen Kelan ylläpitämässä palvelussa tai sen toiminnassa taikka Kelan vastuulle muutoin yhteisrekisterinpitäjänä kuuluvassa toiminnossa, tulee palvelunantajan olla viipymättä yhteydessä Kelaan asian selvittämiseksi. Kela vastaa näissä tilanteissa tietosuoja-asetuksen 33 ja 34 artiklojen mukaisen ilmoitusvelvollisuuden toteuttamisesta. Jos Kelan ylläpitämässä palvelussa tapahtuu tietoturvaloukkaus, joka johtuu muun yhteisrekisterinpitäjän toiminnasta, vastaa ilmoitusvelvollisuuksien toteuttamisesta ensisijaisesti se yhteisrekisterinpitäjä, jonka toiminnassa loukkaus on tapahtunut. Asiasta tulee olla viipymättä yhteydessä myös Kelaan.

Mikäli loukkauksen laatu on sellainen, että se edellyttää yhteisrekisterinpitäjien informointia, rekisterinpitäjät ovat velvollisia ilmoittamaan viipymättä toiselle rekisterinpitäjälle henkilötietojen tietoturvaloukkauksesta, samoin kuin muista seikoista, jotka voivat vaikuttaa toisen osapuolen asiakastietolain 4 §:n tai repseptilain 18 §: perustuvien vastuiden tai velvoitteiden täyttämiseen. Jos tietoturvaloukkaus liittyy myös toisen rekisterinpitäjän

vastuualueeseen kuuluvaan asiaan, tulee tästä informoida rekisterinpitäjää aina loukkauksen ilmetessä ja viipymättä. Ilmoituksen sisältö on määritelty tämän asiakirjan kohdassa 6.4.

6.3.2 Tietoturvaloukkauksen dokumentointi ja toimenpiteet laajenemisen estämiseksi

Yhteisrekisterinpitäjät ryhtyvät aina osaltaan mahdollisen tietoturvaloukkauksen havaitessaan toimiin sen laajenemisen estämiseksi. Tähän liittyen arvioidaan ja tutkitaan, onko tietoturvaloukkaus rajoitettavissa ja voiko se mahdollisesti laajentua. Lisäksi arvioidaan, keille kyseinen loukkaustilanne näkyy ja keiden toimintaan se vaikuttaa. Tässä vaiheessa myös arvioidaan alustavasti, millä edellytyksillä kyseessä olevaa toimintaa voidaan jatkaa. Päätettäviä asioita ovat mm. välittömät toimenpiteet, kuten esim. järjestelmien sulkeminen pois verkosta, jatkuvuussuunnitelmien käyttöönotto ja reagointiin tarvittavat resurssit.

Tärkeä osa mahdollisen tietoturvaloukkauksen käsittelyä on ongelman lähteen määrittäminen. Jos epäillään tai selviää, että kyseessä on esimerkiksi rikos, tietoturvaloukkauksen lähteen selvittäminen on Suomen muun viranomaisen, tällaisessa tapauksessa poliisin tehtävä. Yhteisrekisterinpitäjien tulee dokumentoida tietoturvaloukkaustilanteissa tekemänsä havainnot, toimenpiteet sekä päätökset. Jokainen yhteisrekisterinpitäjä kirjaa omat toimenpiteensä.

Todistusaineistoa on kerättävä ja säilytettävä turvallisesti ja varauduttava siihen, että aineistoa tarvitaan jälkiselvitykseen. Todistusaineiston käsittelyssä turvataan aineiston eheys ja aikaleimat. Todistusaineisto kerätään ja dokumentoidaan mahdollisimman täydellisesti. Todistusaineiston säilytysaika määritellään etukäteen tietoturvaloukkauksen yhteydessä. Tutkinnan varmistamiseksi todistusaineistoa säilytetään kuitenkin vähintään kahden vuoden ajan epäiltäessä tavallista rikosta ja vähintään viiden vuoden ajan epäiltäessä törkeää tai virkarikosta. Mahdollisen rikostutkinnan käynnistyttyä toimitaan poliisin antamien ohjeiden mukaisesti.

6.4 Tietoturvaloukkausilmoituksessa toiselle rekisterinpitäjälle mainittavat tiedot

Ilmoituksessa toiselle yhteisrekisterinpitäjälle tulee olla seuraavat tiedot:

- tietoturvaloukkauksen tunnistenumero (mikäli tällainen on olemassa)
- milloin mahdollinen tietoturvaloukkaus havaittiin ja ilmoitettiin
- onko kyseessä tietosuojaloukkaus
- tietoturvaloukkauksen vaikutus

- tietoturvaloukkauksen nykytila (status, esimerkiksi loukkauksen epäily/vahvistamatta/vahvistettu/korjaustoimenpiteissä oleva tietoturvaloukkaus/selvitetty/raportoitu/käsittely valmis)
- tietoturvaloukkauksen lähde ja syy, jos tiedossa
- tietoturvaloukkauksen kuvaus (minkälaisessa tilanteessa se havaittiin ja mitkä merkit paljastivat mahdollisen tietoturvaloukkauksen)
- kuvaus tietoturvaloukkauksen liittyvistä kohteista (esim. verkot, palvelimet tai verkkopalvelut)
- muut havainnot (esim. poikkeava tietoliikenne, hälytykset tai käyttäjien ilmoitukset)
- tietoturvaloukkauksen priorisointiin vaikuttavat tekijät (mm. tietoturvaloukkauksen kohteena olevan järjestelmän tai tiedon tärkeys)
- vaikutusta pienentävät tekijät (esim. kovalevyn salaus varastetussa tietokoneessa)
- vaikutusta lisäävät tekijät (esim. arkaluonteiseksi luokiteltu tieto)
- tehdyt vastatoimet (esim. estetty tai suodatettu palvelun verkkoliikennettä tai irrotettu työasema verkosta)
- yhteisrekisterinpitäjät, joihin on jo otettu yhteyttä tietoturvaloukkaukseen liittyen

Tietoturvaloukkauksta koskevat tiedot:

- käsittelyn nykyinen tilanne (status)
- tietoturvaloukkauksen yhteenveto
- tietoturvaloukkauksen käsittelyn toimenpiteet ja tarkat ajankohdat
- kaikkien käsittelyyn osallistuneiden yhteystiedot ja tapahtumakirjaukset
- listaus kerätystä todistusaineistosta
- käsittelijän kommentit
- tietoturvaloukkauksen juurisyy
- tietoturvaloukkauksen hallintaan käytetyt kustannukset
- tietoturvaloukkauksen mahdolliset liiketoimintavaikutukset

7. Tietosuoja-asetuksen mukaisen vaikutustenarvion laatiminen

Yhteisrekisterinpitäjät ovat velvollisia arvioimaan tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarvioinnin tarpeellisuuden. Kela laatii yhteisrekisterinpitäjänä oman vaikutustenarvion suorittamistaan käsittelytoimista. Mikäli palvelunantajan käsittely edellyttää tietosuoja-asetuksen artiklan 36 mukaista valvontaviranomaisen ennakkokuulemista, palvelunantaja huolehtii ennakkokuulemismenettelyn toteuttamisesta.

8. Yhteisrekisterinpitäjien yhteistoiminta ja avunanto

Yhteisrekisterinpitäjät huolehtivat osaltaan siitä, että kaikki osapuolet pystyvät täyttämään tietosuojaa koskevat velvollisuutensa ja että rekisteröidyn oikeudet toteutuvat yhteisrekisterinpitäjyydessä täysimääräisesti. Yhteisrekisterinpitäjät vastaavat tahollaan siitä, että tarvittavat yhteystiedot rekisteröidyn oikeuksien käyttämiseksi ovat osapuolten tiedossa ja jatkuvasti ajan tasalla. Yhteisrekisterinpitäjien tulee pitää Kanta-palvelujen asiakasrekisteriin tallentamansa yhteystiedot ajantasaisina.

9. Asiakirjan velvoittavuus ja voimassaolo

Tämä asiakirja on osa Kanta-palvelujen asiakkuuden sitoumusta. Tämä asiakirja tulee voimaan 1.11.2021.

Tämän asiakirjan sisällöstä on pyydetty kommentteja tietyiltä palvelunantajien edustajilta sekä asiaan liittyviltä viranomaistahoilta 1.10.2021 päivätyllä sähköpostiviestillä.