Kela / Kanta-palvelut
1.1.2024

# 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 käsittelystä annetun lain (703/2023, jäljempänä asiakastietolaki) 70–72 §:ien sekä sähköisestä lääkemääräyksestä annetun lain (61/2007, jäljempänä lääkemääräyslaki) 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 ja tiedonhallintapalvelun osalta yhteisrekisterinpitäjiä, joita ovat Kansaneläkelaitos (jäljempänä Kela) sekä sosiaali- ja terveydenhuollon palvelunantajat. Reseptikeskuksen osalta tämä asiakirja 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 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.

Tässä asiakirjassa käsiteltävän yhteisrekisterinpitäjyyden osalta on huomioitava, mitä asiakastietolaissa on yhteisrekisterinpitäjyyden vastuista erikseen säädetty. Asiakastietolain 70 §:n mukaan kukin sosiaali- ja terveydenhuollon palvelunantaja ja Kansaneläkelaitos ovat sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien yhteisrekisterinpitäjiä, jolloin vastuunjako määräytyy seuraavasti:

- Lokirekisterien säilytyspalvelun tietoja tallentavat palvelunantajat vastaavat toiminnassaan syntyneiden tietojen oikeellisuudesta sekä muista rekisterinpitäjän velvoitteista.
- Kansaneläkelaitos vastaa yhteisrekisterinpitäjänä tietojen turvallisuuden varmistamisesta sekä tietojen säilyttämisestä ja hävittämisestä siten kuin 66 §:ssä säädetään. Kansaneläkelaitos toimii tietosuoja-asetuksen 26 artiklan 1 kohdan mukaisena yhteyspisteenä.

Asiakastietolain 71–72 §:n mukaisesti kukin sosiaali- ja terveydenhuollon palvelunantaja ja Kela ovat tiedonhallintapalvelun sekä tahdonilmaisupalvelun yhteisrekisterinpitäjiä, jolloin vastuunjako määräytyy seuraavasti:

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

Reseptilain 18 §:n 1 momentin 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.

- 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.
- Sähköisiä lääkemääräyksiä laativa palvelunantaja ja itsenäinen lääkkeen määrääjä vastaavat Reseptikeskukseen tallennettavan lääkemääräyksen tietojen oikeellisuudesta.
- Lääkkeen toimittanut apteekki vastaa Reseptikeskukseen tallennettavien toimitustietojen oikeellisuudesta.

Edellä mainittujen palvelujen lisäksi asiakastietolaissa on säädetty ammattilaisen käyttöliittymän käyttölokien (70 §, Kelain-palvelu) sekä toimintansa lopettaneiden palvelunantajien asiakasasiakirjojen yhteisrekisterinpitäjyydestä (16 §). Kyseessä olevia yhteisrekisterinpitäjyystilanteita ei käsitellä tässä asiakirjassa, vaan näiden osalta annetaan omat ohjeistukset.

## 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 viitataan tietosuoja-asetuksen mukaisiin määritelmiin.

Sosiaali- ja terveydenhuollon palvelunantajalla tarkoitetaan tässä asiakirjassa palvelunantajaa, joka on liittynyt Kanta-palvelujen käyttäjäksi ja näin ollen käyttää asiakastietovarantoa, tiedonhallintapalvelua sekä tahdonilmaisupalvelua tai Reseptikeskusta.

## 3. Palvelujen kuvaukset ja niissä käsiteltävät henkilötiedot

### 3.1 Tiedonhallintapalvelu

Tiedonhallintapalvelu on asiakastietolain yksi 65 §:ssä mainituista valtakunnallisia tietojärjestelmäpalveluista. Tiedonhallintapalvelu koostaa vain potilastietoja. Tiedonhallintapalvelu koostaa potilasasiakirjoista terveydenhuollon toteuttamisen kannalta

keskeiset ajantasaiset potilastiedot ja tuottaa niistä yhteenvetoja palvelunantajille ja apteekeille 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. Tiedonhallintapalvelu saa koostaa myös muita potilasasiakirjamerkintöjä.

Sosiaali- ja terveydenhuollon palvelunantajan oikeus käsitellä tiedonhallintapalveluun tallennettuja tietoja määräytyy asiakastietolain 53 – 54 §:n mukaisesti. Tiedonhallintapalvelusta saatujen tietojen käsittelyssä on lisäksi huomioitava, mitä asiakastietolain 9 §:ssä on käyttöoikeuksista erikseen säädetty.

### 3.2 Tahdonilmaisupalvelu

Tahdonilmaisupalvelu on asiakastietolain yksi 65 §:ssä mainituista Kanta-palveluista. Asiakastietolain 58 ja 72 §:n mukaisesti tahdonilmaisupalveluun on tallennettava viivytyksettä tieto henkilölle annetusta asiakastietolain ja lääkemääräyslain 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. Tällaisia tahdonilmaisuja ovat esimerkiksi hoitotahtoa ja elinluovutustahtoa koskevat asiakirjat.

### 3.3 Sosiaali- ja terveydenhuollon luovutuslokit

Palvelunantajan on kerättävä lokitiedot asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja luovutuksesta seurantaa ja valvontaa varten (asiakastietolain 10 §). Sosiaali- ja terveydenhuollon luovutuslokilla tarkoitetaan lokia, joka sisältää tiedot henkilötietojen luovutuksesta eri rekisterien tai rekisterinpitäjien välillä.

Luovutuslokirekisteriin tallennetaan kuvaus luovutetuista asiakastiedoista sekä tieto siitä palvelunantajasta, jonka asiakastietoja luovutetaan, asiakastietojen luovuttajasta, luovutuksen saajasta, luovutusajankohdasta, käyttötarkoituksesta, johon tiedot on luovutettu

sekä luovutuksen perusteena oleva säännös taikka luovutuslupaa tai suostumusta koskevat tiedot sekä muut luovutusten valvontaa ja seurantaa varten tarvittavat tiedot.

### 3.4 Reseptikeskus

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

## 4. Henkilötietojen käsittelyperuste ja oikeus henkilötietojen käsittelyyn

Palveluantajat voivat käsitellä tiedonhallintapalveluun tietoja lähtökohtaisesti vain potilaan hoidon tai palvelun toteuttamista varten. Asiakkaan antamista luovutusluvasta, suostumuksesta ja kielloista on säädetty muun ohella asiakastietolain 8 luvussa. Samassa yhteydessä on säädetty asiakastietojen luovuttamisesta ja luovuttamisen edellytyksistä valtakunnallisten tietojärjestelmäpalvelujen välityksellä sekä muulla tavoin. Reseptikeskukseen tallennettujen tietojen luovuttamisesta on säädetty lisäksi erikseen lääkemääräyslain 13 §:ssä. Tahdonilmaisupalveluun tallennettujen tahdonilmaisujen käsittelyä on tarkemmin käsitelty potilastiedon arkiston toimintamallissa[1] ja sosiaalihuollon osalta Kanta-palvelujen käsikirjassa sosiaalihuollon toimijoille.[2]

Reseptikeskuksen osalta apteekit voivat käsitellä Reseptikeskukseen tallennettuja tietoja lääkemääräyksen toimittamista ja tähän liittyviä tehtäviä varten. Apteekkien tiedonsaantioikeudesta on säädetty reseptilain 11 §:ssä. Sosiaali- ja terveydenhuollon palvelunantaja sekä lääkkeen määrääjät voivat käsitellä Reseptikeskuksen tietoja potilaan hoidon ja lääkityksen seurantaa ja toteuttamista varten. Reseptikeskuksen tietojen luovuttamisesta ja kielto-oikeudesta on säädetty lääkemääräyslain 13 §:ssä.

Tässä asiakirjassa tarkoitettujen yhteisrekistereihin tallennettujen henkilötietojen käsittelyperuste on lainsäädäntö. Käyttöoikeudesta asiakastietoon on säädetty asiakastietolain 15 §:ssä sekä sen nojalla annettavassa asetuksessa ja sähköisten

[1] https://yhteistyotilat.fi/wiki08/display/JULPOAR
[2] Kanta-palvelujen käsikirja sosiaalihuollon toimijoille - Kanta-palvelujen käsikirja sosiaalihuollon toimijoille - Oma työpöytä (yhteistyotilat.fi)

lääkemääräystietojen osalta lääkemääräyslain 4 luvussa. Tässä asiakirjassa tarkoitettuihin palveluihin tallennettuja henkilötietoja ei siirretä EU:n/ETA:n ulkopuolelle. Lisäksi pilvipalveluiden turvallisuuden arviointikriteerit (jatkossa PiTuKri) [3] edellyttävät, että yhteiskunnan kannalta kriittisen toiminnan kannalta olennaisen tietojärjestelmän on oltava Suomessa. Lisäksi arkaluontoisten henkilötietojen keskittymän on oltava Suomessa. Mikäli tietojärjestelmä tarjotaan esimerkiksi joltain osin pilvipalveluna, edellä mainitut PiTuKri:n vaatimukset on soveltuvin osin 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 lääkemääräyslaissa säädetyn vastuunjaon mukaisesti. 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 (sisältäen Reseptikeskuksen luovutuslokit): sosiaali- ja terveydenhuollon palvelunantajat, itsenäiset lääkkeen määrääjät, apteekit sekä Kela.

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

### 5.2 Rekisteröidyn informointi ja rekisteröidyn oikeuksien käyttäminen

Kela toimii asiakastietolain sekä lääkemääräyslain mukaan tiedonhallintapalvelun, tahdonilmaisupalvelun, sosiaali- ja terveydenhuollon luovutuslokien sekä Reseptikeskuksen

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

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. Tiedonhallintapalvelun tarkastusoikeus ei koske tiedonhallintapalvelun potilasasiakirjoilta koostamia potilasasiakirjoja, koska näitä tietoja ei ole ensisijaisesti tallennettu tiedonhallintapalveluun. Näiden osalta tarkastuspyynnön toteuttamisesta vastaa se palvelunantaja, jonka toiminnassa tiedot ovat syntyneet.

Kela vastaa yhteisrekisterinpitäjänä tiedonhallintapalvelun luovutuslokitietojen luovuttamisesta. Mikäli rekisteröity käyttää tarkastusoikeuttaan suhteessa mainittuihin tiedonhallintapalveluun tallennettuihin tietoihin, vastaa Kela tarkastuspyynnön toteuttamisesta ja siitä, että rekisteröidylle kuuluva oikeus saada pääsy tietoihin toteutuu, koska asiakastietolain 71 §:n mukaisesti Kela vastaa yhteisrekisterinpitäjänä tietojen luovuttamisesta. Kela toimittaa rekisteröidylle hänestä tiedonhallintapalveluun tallennetut tiedot tietosuoja-asetuksen mukaisesti. Rekisteröidyn on mahdollista katsella tiedonhallintapalveluntietoja 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 suhteessa tahdonilmaisupalveluun tallennettuihin tietoihin, vastaa Kela tarkastuspyynnön toteuttamisesta ja siitä, että rekisteröidylle kuuluva oikeus saada pääsy tietoihin toteutuu, koska asiakastietolain 72 §:n mukaisesti Kela vastaa yhteisrekisterinpitäjänä tietojen luovuttamisesta. Kela toimittaa rekisteröidylle hänestä tallennetut tiedot tietosuoja-asetuksen mukaisesti. Rekisteröidyn on mahdollista katsella, muokata sekä poistaa häntä koskevia tahdonilmaisuja kootusti OmaKanta-palvelun kautta.

*5.3.3 Reseptikeskus*

Rekisteröidyllä on oikeus tarkastaa hänestä Reseptikeskukseen tallennetut tiedot. Reseptikeskuksen osalta potilaan tiedonsaantioikeudesta ja tietojen korjaamisesta säädetään tietosuoja-asetuksessa sekä lokitietojen tiedonsaantioikeudesta osalta asiakastietolaissa. Lääkemääräyksen korjaamisesta, lopettamisesta, mitätöinnistä ja uudistamisesta säädetään lisäksi lääkemääräyslain 10 §:ssä. Jos potilas tai hänen laillinen edustajansa vaatii tiedon oikaisua tai korjaamista ja virheellinen tieto perustuu lääkkeen määrääjän tai lääkkeen toimittajan tekemään merkintään, vaatimus oikaisemisesta on osoitettava merkinnän tehneelle henkilölle tai sille organisaatiolle, jonka palveluksessa kyseisen merkinnän tehnyt henkilö on ollut merkinnän 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.

*5.3.4 Sosiaali- ja terveydenhuollossa syntyneet luovutuslokitiedot sekä muut luovutuslokitiedot*

Asiakastietolain 70 §:n 5 momentin mukaan Kela ja palveluantaja ovat sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien yhteisrekisterinpitäjiä. Kela vastaa yhteisrekisterinpitäjänä tietojen turvallisuuden varmistamisesta sekä tietojen säilyttämisestä ja hävittämisestä siten kuin asiakastietolain 66 §:ssä säädetään. Tältä osin palvelunantajan, jonka toiminnassa luovutuslokimerkintä on syntynyt, vastaa tallentuneen tiedon oikeellisuudesta sekä siihen liittyvistä tarkastuspyynnöistä.

Luovutuslokitietojen osalta on huomioitava, että asiakastietolain 11 §:n 1 momentin mukaisesti asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten muun muassa palvelunantajalta, kirjallisesta pyynnöstä kohtuullisessa ajassa ja viimeistään kahden kuukauden kuluessa maksutta tieto siitä muun ohella siitä, kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste.

Lähtökohtaisesti asiakkaan on mahdollista tarkastella luovutuslokitietoja OmaKanta-palvelun välityksellä. Mikäli asiakas tarvitsee lisätietoja asiakastietojensa luovutuksiin liittyen, tulee asiakkaan olla yhteydessä siihen palvelunantajaan, jonka asiakastietoja on luovutettu tai jolle niitä on luovutettu.

Reseptikeskuksen luovutuslokitietojen osalta on huomioitava, että Kela vastaa lääkemääräyslain 18 §:n mukaisesti Reseptikeskukseen tallennettujen tietojen luovuttamisesta. Näin ollen asiakastietolain 11 §:n mukaisesti asiakkaalla on oikeus saada Kelalta kirjallisesta pyynnöstä kohtuullisessa ajassa ja viimeistään kahden kuukauden kuluessa maksutta tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia Reseptikeskukseen tallennettuja tietoja sekä mikä on ollut käytön tai luovutuksen peruste.

Asiakkaalla ei kuitenkaan ole oikeutta saada lokitietoja, jos sen, jolta niitä pyydetään, tiedossa on, että niiden antamisesta saattaisi aiheutua vakavaa vaaraa asiakkaan terveydelle tai

hoidolle taikka jonkun muun oikeuksille tai jos niiden antaminen saattaisi vaarantaa rikosten estämisen, paljastamisen ja selvittämisen taikka yleisen turvallisuuden tai kansallisen turvallisuuden suojelemisen. Myöskään kahta vuotta vanhempia lokitietoja ei ole oikeutta saada, jollei siihen ole erityistä syytä. Asiakas ei saa käyttää tai luovuttaa saamiaan lokitietoja edelleen muuhun tarkoitukseen kuin omien asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä ja toteuttamista varten.

Jos palvelunantaja, Kela tai apteekki katsoo, ettei lokitietoja saa antaa asiakkaalle, kieltäytymisestä on tehtävä kirjallinen päätös. Asia voidaan saattaa tietosuojavaltuutetun käsiteltäväksi tietosuojalain 21 §:n 1 momentin mukaisesti. Asian arviointi kuuluu sille taholle, joka on toimivaltainen asiakkaan esittämän pyynnön käsittelyyn. Toimivaltainen taho määräytyy riippuen siitä, mitä tietoja asiakkaan pyyntö koskee.

Jos asiakas pyytää uudestaan lokitietoja, jotka hän on jo saanut, palvelunantaja ja Kela voi periä lokitietojen antamisesta kohtuullisen korvauksen, joka ei saa ylittää tiedon antamisesta aiheutuvia välittömiä kustannuksia. Pääsystä lokitietoihin 74 §:ssä tarkoitetun OmaKannan avulla ei kuitenkaan saa periä maksua.

Tiedot on annettava viivytyksettä. Jos palvelunantaja tai Kela katsoo, ettei lokitietoja saa antaa asiakkaalle, kieltäytymisestä on tehtävä kirjallinen päätös. Asia voidaan saattaa tietosuojavaltuutetun käsiteltäväksi tietosuojalain 21 §:n 1 momentin mukaisesti.

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 käyttöä koskeva merkintä on syntynyt (asiakastietolain 70 §). Lisäksi asiakastietolain 74 §:n 2 momentin mukaisesti rekisteröidylle saadaan näyttää OmaKanta-palvelun välityksellä hänen tietojensa käsittelyä koskevat luovutus- ja käyttölokitiedot lukuun ottamatta luovutuksensaajan henkilötietoja.

Sosiaali- ja terveydenhuollossa sekä apteekeissa syntyneiden käyttölokien osalta on huomioitava, että asiakastietolain 70 §:n 3 momentin mukaan kukin sosiaali- ja terveydenhuollon palvelunantaja, apteekki ja Kansaneläkelaitos ovat toiminnassaan syntyneiden käyttölokien rekisterinpitäjiä. Näin ollen tässä asiakirjassa käsitellyt vastuunjaot eivät koske toiminnassa syntyneitä käyttölokitietoja.

## 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 artiklojen mukaisesti. Reseptikeskuksen osalta vastuutaho on lääkkeen toimittanut apteekki, mikäli kyseinen pyyntö kohdistuu lääkkeen toimitustietoihin. 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 asiakastietolain sekä lääkemääräyslain liitteissä. Tietosuoja-asetuksen 17 artiklan 3 kohdan näkökulmasta on huomioitava, ettei rekisteröidyn oikeutta poistaa häntä koskevat tiedot sovelleta, kun käsittely on tarpeen rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Näin ollen sosiaali- ja terveydenhuollossa rekisteröidyllä ei ole oikeutta saada häntä koskevia asiakirjoja tai niiden sisältämiä tietoja taikka näitä koskevia lokitietojaan poistetuksi ennen laissa säädetyn säilytysajan päättymistä.

## 5.5 Palvelunantajan ja apteekin oikeus saada yhteisrekisterinpitäjyyteen liittyviä tietoja Kelalta

Edellä mainittujen rekisteröityjen oikeuksien toteuttamisen näkökulmasta voi olla tarpeen lisäksi huomioida, mitä erikseen asikastietolaissa on säädetty palvelunantajan sekä apteekin oikeudesta saada lokitietoja Kelalta. Yksityisen terveydenhuollon osalta tietoja on mahdollista luovuttaa palvelunantajan lukuun toimivalle rekisterien tekniselle ylläpitäjälle, mikäli luovutuksen edellytykset täyttyvät. Edellä mainittuun liittyen on huomioitava alla mainitut asiakastietolain säännökset.

Asiakastietolain 66 §:n 3 momentin 4 kohdan mukaan Kelalla on oikeus antaa tahdonilmaisupalvelussa olevia luovutusten hallintaan liittyviä asiakirjoja ja niiden lokitietoja sosiaali- ja terveydenhuollon palvelunantajille asiakastietojen käytön ja luovutuksen seurantaa ja valvontaa varten, jos on ilmeistä, ettei siten vaaranneta turvajärjestelyjen toteutumista. Saman pykälän 5

momentin mukaan Kela voi laatia ja luovuttaa palvelunantajalle sen omassa rekisterissä oleviin, valtakunnallisiin tietojärjestelmäpalveluihin tallennettuihin asiakastietoihin ja lokitietoihin perustuvia yhteenvetoja, joilla on merkitystä palvelunantajan toiminnan kehittämisessä, seurannassa, raportoinnissa ja valvonnassa. Nämä yhteenvedot eivät saa sisältää henkilötietoja.

Lisäksi asiakastietolain 78 §:n 2 momentin mukaan tietosuojan ja tietoturvan seurannan ja valvonnan toteuttamiseksi palvelunantajalla ja apteekilla on oikeus saada Kelalta omien asiakasrekisteriensä lokitiedot, tiedonhallintapalvelussa ja tahdonilmaisupalvelussa olevien tietojen käsittelyyn liittyvät lokitiedot ja omatietovarannon lokitiedot siltä osin kuin asianomaisen palvelunantajan tai apteekin henkilökunta on katsellut ja käsitellyt asiakkaan tiedonhallintapalvelussa, tahdonilmaisupalvelussa ja omatietovarannossa olevia tietoja, jos se on tarpeen asiakkaan asiakastietojen käsittelyn lainmukaisuuden selvittämiseksi.

## 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 82 §: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 merkittävä poikkeama olennaisissa vaatimuksissa. Kyseessä olevassa tilanteessa tietojärjestelmän valmistajalla sekä ja

apteekilla on asiakastietolain 82 §:n mukaisesti velvollisuus ilmoittaa asiasta Sosiaali- ja terveysalan lupa- ja valvontavirastolle ja Kelalle. Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.

Asiakastietolain 90 §:n mukaisesti, jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kelan tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä.

Yhteisrekisterinpitäjät vastaavat siitä, että ne kykenevät omassa toiminnassaan havaitsemaan mahdolliset tietoturvaloukkaustilanteet sekä tietojärjestelmän merkittäviin poikkeamiin liittyvät tilanteet riittävän nopeasti sekä siitä, että tähän liittyvä havainnointi on sisällytetty yhteisrekisterinpitäjän omiin ohjeistuksiin sekä menettelytapoihin.

## 6.2 Vastuunjako eri palveluissa

Tiedonhallintapalvelun ja tahdonilmaisupalvelun osalta palvelunantajat vastaavat asiakastietolain 71–72 §:n mukaisesti muista rekisterinpitäjälle kuuluvista velvoitteista. Näin ollen johtava vastuu näiden palveluiden henkilötietojen tietoturvaloukkausten ilmoittamisesta on kyseessä olevalla palvelunantajalla. Yhteisrekisterinpitäjät kuitenkin vastaavat aina ensisijaisesti omassa toiminnassaan tapahtuneista tai epäillyistä tietoturvaloukkauksista. Sosiaali- ja terveydenhuollossa syntyneiden luovutuslokien, tiedonhallintapalvelun sekä tahdonilmaisupalvelun osalta Kela vastaa yhteisrekisterinpitäjänä tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja tuhoamisesta asiakastietolain 66 § mukaisesti. Lisäksi 66 §:n osalta on huomioitava, mitä Kelan vastuista ja oikeuksista on Kanta-palvelujen järjestäjänä erikseen säädetty. Edellä mainituin osin Kela vastaa yhteisrekisterinpitäjänä myös palvelussa ilmenevistä mahdollisista tietoturvaloukkauksista sekä siihen liittyvästä ilmoitusmenettelyn toteuttamisesta.

Myös Reseptikeskuksen osalta Kelalla on ensijainen vastuu tietoturvaloukkausilmoitusmenettelyn toteuttamisesta, mikäli loukkausepäilyn katsotaan aiheutuneen Kanta-palvelujen toiminnasta. Tämän lisäksi Kela vastaa lääkemääräyslain 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 viimesijainen

vastuu Reseptikeskuksen henkilötietojen tietoturvaloukkausten ilmoittamisesta on Kelalla. Mikäli Reseptikeskukseen tallennettuihin tietoihin kohdistuva tietoturvaloukkaus tapahtuu muun yhteisrekisterinpitäjän omassa toiminnassa, kuten reseptitietojen käsittelyssä, ensisijainen vastuu ilmoitusvelvollisuuden toteuttamisesta on sillä yhteisrekisterinpitäjällä, jonka toiminnassa epäilty loukkaus on tapahtunut.

### *6.2.1 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, loukkaus jatkoselvitetään ja ratkaistaan kyseessä olevan yhteisrekisterinpitäjän toimesta. 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 loukkauksesta viipymättä toisilleen. Tarvittaessa yhteisrekisterinpitäjät voivat informoida toisiaan myös epäillyistä tietoturvaloukkaustilanteesta. 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. Mikäli loukkaus todetaan tapahtuneeksi, 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 yhteisrekisterinpitäjän toiminnassa tapahtuneen loukkauksen laatu edellyttää, rekisterinpitäjät ovat velvollisia ilmoittamaan viipymättä toiselle rekisterinpitäjälle kyseessä olevasta tietoturvaloukkauksesta tai sen epäilystä, samoin kuin muista seikoista, jotka voivat vaikuttaa toisen osapuolen asiakastietolain tai lääkemääräyslain mukaisten vastuiden tai velvoitteiden täyttämiseen. Jos loukkaus 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.

### *6.2.2 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.

### 6.3 Tietoturvaloukkausilmoituksessa toiselle rekisterinpitäjälle mainittavat tiedot

**Ilmoituksessa toiselle yhteisrekisterinpitäjälle tulee olla mahdollisimman kattavasti seuraavat tiedot:**

- tietoturvaloukkauksen mahdolliset tunnistenumerot
- milloin mahdollinen tietoturvaloukkaus havaittiin ja/tai ilmoitettiin
- onko kyseessä tietosuojaloukkaus
- henkilötieto ja rekisteri, johon tietoturvaloukkaus kohdistuu
- tietoturvaloukkauksen
    - tietoturvaloukkauksen nykytila (status, esimerkiksi loukkauksen epäily/vahvistamatta/vahvistettu/korjaustoimenpiteissä oleva tietoturvaloukkaus/selvitetty/raportoitu/käsittely valmis)
- miten henkilötietojen tietoturvaloukkaus havaittiin
- kuvaus tietoturvaloukkauksesta
    - 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)
- tapa, jolla loukkaus voi vaikuttaa rekisteröityihin
- kohteena olevat rekisteröidyt
- tallenteiden lukumäärä
- rekisteröityjen lukumäärä
- suunnitelma jatkotoimenpiteistä / toteutetut ja ehdotetut toimenpiteet

- 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

**Tietoturvaloukkausta koskevat tiedot:**

- käsittelyn nykyinen tilanne (status)
- tietoturvaloukkauksen yhteenveto
- tietoturvaloukkauksen käsittelyn toimenpiteet ja tarkat ajankohdat
- käsittelyyn osallistuneiden yhteystiedot ja tarvittavat tapahtumakirjaukset
- listaus kerätystä todistusaineistosta
- tietoturvaloukkauksen juurisyy

### 6.4 Tietoturvaloukkausilmoituksessa toiselle rekisterinpitäjälle mainittavat tiedot

Ilmoituksessa toiselle yhteisrekisterinpitäjälle annettaan seuraavat tiedot:

- yhteyshenkilö(t) yhteystietoineen (nimi, tehtävä, puhelin, osoite)
- yhteyshenkilön sähköpostiosoite
- tietoturvaloukkauksen tunnistenumero (organisaation oma tunnus tietoturvaloukkaukselle, mikäli tällainen on olemassa)
- muut osalliset tai tahot (yhteisrekisterinpitäjä, henkilötietojen käsittelijä, muu osallinen), yhteystiedot
- miten ja milloin tietoturvaloukkaus havaittiin
  - tietoturvaloukkauksen alkamispäivämäärä
  - tietoturvaloukkauksen päättymispäivämäärä tai arvio päättymisestä
- kuvaus tietoturvaloukkauksesta
  - luvaton luovuttaminen tai pääsy tietoihin
  - tietojen muuttaminen
  - tietojen lainvastainen tai vahingossa tapahtunut tuhoaminen tai hävittäminen
  - tietojen saatavuus tai käytettävyys on tilapäisesti estynyt tai
  - muu tapahtuma, joka on johtanut tietoturvaloukkaukseen
- tietoturvaloukkauksen tapa
- tietoturvaloukkauksen syy

- tietoturvaloukkauksen kohteena olevat rekisteröidyt ja lukumäärä
- arvio mahdollisten vaikutusten vakavuudesta rekisteröidyille
- mikä on tietoturvaloukkauksen selvityksen tilanne esimerkiksi
    - epäily loukkauksesta on vahvistamatta/vahvistettu
    - korjaustoimenpiteissä oleva tietoturvaloukkaus on selvitetty/raportoitu/valmis)
    - suunnitelma jatkotoimenpiteistä
- toteutetut toimenpiteet tietoturvaloukkauksen estämiseksi ja/tai tehdyt vastatoimet
- tieto, jos tietoturvaloukkauksesta on ilmoitettu valvontaviranomaiselle (kyllä / ei)
- tieto, jos tietoturvaloukkauksesta on ilmoitettu rekisteröidylle (kyllä / ei)
- yhteisrekisterinpitäjät, joille on ilmoitettu tietoturvaloukkauksesta
- onko tietoturvaloukkauksen kohteella toimipaikkoja tai järjestelmien riippuvuuksia EU/ETA-maissa? (kyllä / ei)
- onko tietoturvaloukkauksen kohteella henkilötiedon siirtoa EU/ETA-maiden ulkopuolelle? (kyllä / ei)

## 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. 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. Asiakirja korvaa asiaa koskevan aiemmin annetun asiakirjan. Tämä asiakirja tulee voimaan 1.1.2024.