HENKILÖTIETOJEN KÄSITTELY

Ulkopuoliset palveluntuottajat

(Saarikan sidosryhmät mm. palvelusetelituottajat, yksityiset palveluntuottajat ja kunnat)

SoTe ky/Perusturvaliikelaitos Saarikan hallinnon ohje

03/2019

Hyväksytty Liikelaitoksen johtajan viranhaltijapäätöksellä 28.3.2019 §2.

Sisällys

1. JOHDANTO 3
2. ORGANISOINTI JA VASTUU 3
3. HENKILÖTIETOJEN KÄSITTELYSÄÄNNÖT 4
4. HENKILÖTIEDON ELINKAARI 5
5. REKISTERÖIDYN OIKEUDET 7
6. REKISTERINPITÄJÄ (Saarikka) 9
7. PALVELUNTUOTTAJA (henkilötietojen käsittelijä) 10
8. KESKEINEN TERMINOLOGIA 15
9. HENKILÖTIETOJEN KÄSITTELYÄ OHJAAVIA LAKEJA, ASETUKSIA ja SUOSITUKSIA 16

Julkinen ohje perustuu EU:n tietosuoja-asetukseen (2016/679), jota sovelletaan sekä automaattiseen että manuaalisesti suoritettavaan henkilötietojen käsittelyyn.

1. JOHDANTO

Viiden eri kunnan (Saarijärvi/Pylkönmäki, Karstula, Kannonkoski, Kyyjärvi ja Kivijärvi) alueella toimivan Sote kuntayhtymän pääasiallisena tehtävänä on järjestää jäsenkuntien ja mahdollisten sopimuskuntien puolesta kaikki kuntien järjestettäväksi antamat sosiaalihuollon, perusterveydenhuollon ja erikoissairaanhoidon palvelut. Palvelujen tuottajana toimii lähtökohtaisesti kuntayhtymän tuotanto-organisaatioksi perustettu **kuntayhtymän liikelaitos Saarikka.**

Saarikka tuottaa palveluja itse tai se hankkii ne esim. yksityisiltä palveluntuottajilta, palvelusetelituottajilta tai kunnilta. Saarikka toimii pääsääntöisesti ostopalvelujensa rekisterinpitäjänä.

25.5.2018 voimaan tullut **EU:n yleinen tietosuoja-asetus (EU) 2016/679** velvoittaa sekä Saarikkaa rekisterinpitäjänä, että sen henkilötietojen käsittelijöitä ja näiden mahdollisia alihankkijoita, jotka tuottavat Saarikan järjestämisvelvoitteeseen kuuluvia palveluja.

Henkilötietojen käsittelijöillä tarkoitetaan tässä ohjeessa Saarikan ulkopuolisia palveluntuottajia.

Rekisterinpitäjänä Saarikan tulee ohjeistaa kirjallisesti henkilötietojen käsittelijöitään, myös ulkopuolisia. Tämä ohje koskee kaikkia niitä sidosryhmiä, joille Saarikka on ulkoistanut henkilötietojen käsittelyä.

Saarikka linjaa, että ulkopuoliset palveluntuottajat noudattavat ja soveltavat Saarikan toimintaan ja tehtäviin liittyviä lakeja ja ohjeistuksia myös asiakirjahallintoon, arkistotoimeen sekä tietosuoja-asetukseen liittyen. Ulkoisia palveluja Saarikalle tuotettaessa, palveluntuottajia koskevat aivan samat lait, määräykset ja ohjeistukset kuin Saarikan omassa palvelutuotannossakin.

Ulkopuolisille palveluntuottajille on laadittu erillinen Saarikan asiakirjojen käsittelyohje 02/2019. Se löytyy Saarikan internetsivuilta palveluntuottajien osiosta.

Solmittavilla sopimuksilla ja erillisillä ohjeilla Saarikka ohjeistaa henkilötietojen käsittelijöitään toimimaan vastuullisesti; käsittelijän tulee sitoutua sopimukseensa ja hyväksyä Saarikan toiminta rekisterinpitäjänä.

Tietosuoja-asetuksen mukaisesti Saarikka saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka huolehtivat asianmukaisista suojatoimista ja varmistavat, että käsittely täyttää tietosuoja-asetuksen vaatimukset. Näin varmistetaan rekisteröidyn oikeuksien suojelu.

Saarikalla on oikeus tarvittaessa muuttaa ja täydentää antamiaan ohjeitaan.

Saarikka sitoutuu pitämään salassa palveluntuottajan liike- ja ammattisalaisuudet.

TUTUSTUMALLA alla olevaan linkkiin tietosuojavaltuutetun nettisivuille saa arvokasta lisätietoa:

https://tietosuoja.fi/henkilotietojen-kasittelijat

2. ORGANISOINTI JA VASTUU

Saarikka omistaa tämän ohjeen ja vastaa sen ylläpitämisestä.

Saarikan tietoturvatyöryhmä on käsitellyt arkistosihteeri/tietosuojavastaavan laatiman ohjeen 11/2018. Liikelaitoksen johtaja on hyväksynyt käytettäväksi tätä ohjeena ulkopuolisille palveluntuottajille, jotka tuottavat Saarikan palveluja ja toimivat Saarikan henkilötietojen käsittelijöinä.

Sopimusten tekemisestä vastaava huolehtii tämän ohjeen saattamisesta henkilötietojen käsittelijöiden tietoon sopimuksen solmimisen yhteydessä tai toiminnan edelleen jatkuessa. Ohje löytyy myös Saarikan internetsivuilta palveluntuottajien omasta osiosta.

3. HENKILÖTIETOJEN KÄSITTELYSÄÄNNÖT

Saarikan henkilötiedoissa on kyse viranomaiselle kuuluvista henkilötiedoista. Saarikan eri henkilörekisterit muodostuvat sosiaalihuollon, terveydenhuollon ja erilaisten hallinnollisten tukipalveluiden aineistoista. Tietojen käsittely perustuu kansalliseen lainsäädäntöön ja kansallisiin määrityksiin. Rekisterien omistaja on rekisterinpitäjänä Saarikka, joka määrittää henkilötietojen käsittelyn tarkoitukset ja keinot. Palveluntuottajan muodostamat henkilörekisterit ovat Saarikan ”osarekistereitä”, joissa muodostuviin tietoihin Saarikalla on myös arkistointivelvoite.

Palveluntuottajan tulee noudattaa voimassa olevan tietosuojalainsäädännön edellyttämiä menettelytapoja ja henkilötietojen käsittelyä ja suojaamista koskevia säännöksiä. Palveluntuottaja vastaa myös siitä, että palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön ja Saarikan kanssa solmitun sopimuksen vaatimusten mukainen.

3.1 Henkilötietojen käsittelyn oikeusperusta/vaatimustenmukaisuus

Henkilötietojen rekisteröinti perustuu Saarikan lakisääteisten velvoitteiden täyttämiseen *(tietosuoja-asetuksen artikla 6, kohta 1*). Säännöstöä tulee henkilötietojen käsittelijän noudattaa omaan toimintaansa soveltaen.

Tärkeimmät lait ohjeen lopussa.

3.2 Käsittelyn periaatteet *(asetuksen artiklat 5 ja 25)*

Palveluntuottajan tulee noudattaa asetuksen velvoittamia periaatteita käsitellessään Saarikan henkilötietoja. Ne on otettava huomioon kaikessa henkilötietojen käsittelyssä.

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.

3.3 Käsittelyn lailliset perusteet *(artiklat 6-8)*

Käsittelylle on aina oltava lainsäädännössä säädetty käsittelyperuste. Henkilötietoja saa käsitellä ainoastaan asetuksessa säädetyllä perusteella:

- suostumus rekisteröidyltä
- Saarikan tai kolmannen osapuolen oikeutettu etu
- sopimukseen perustuva käsittely
- lakiin perustuva käsittely
- muut henkilötietojen käsittelyyn liittyvät lailliset perusteet (elintärkeiden etujen suojaaminen/julkinen valta)

3.4 Erityisten henkilötietoryhmien käsittely *(artikla 9)* = ***arkaluonteiset tiedot***

Saarikan aineistot ovat pääsääntöisesti salassa pidettäviä ja arkaluonteisia, erityisiin henkilötietoryhmiin kuuluvia. Niitä koskee myös hyväksikäyttökielto ja vaitiolovelvollisuus, joka voi olla laajempi kuin salassapitovelvollisuus, koska se koskee myös tietoja joita ei ole tallennettu. Viranomaisen asiakirjan salassa pidosta säätää Julkisuuslaki (621/1999) §24.

Salassa pidettävien aineistojen käsittely vaatii erityistä tarkkuutta ja osaamista myös käsittelijöiltä. Vastuu ja mahdolliset, olemassa olevat riskit kyseisten aineistojen käsittelyssä on tärkeä tiedostaa.

Saarikan palveluntuottajana toimiva ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutenkaan toiminnassaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa senkään jälkeen, kun toiminta tai tehtävän hoitaminen Saarikan lukuun on päättynyt. Sama vaatimus koskee myös harjoittelijoita ja palveluntuottajan muuta henkilökuntaa. Salassapitosopimuksen allekirjoittaminen koskee myös palveluntuottajaa ja hänen henkilökuntaansa.

4. HENKILÖTIEDON ELINKAARI

Henkilötietoja käsittelevänä organisaationa Saarikan on vastattava ja kyettävä osoittamaan koko tiedon elinkaaren ajan, että se noudattaa toiminnassaan henkilötietojen käsittelyn periaatteita. Seuraavassa kuvataan keskeiset henkilötiedon elinkaaren vaiheet ja niihin liittyvät toiminnot.

4.1 Kerääminen

Tietoa on hyväksyttävää kerätä ainoastaan määrättyä tarkoitusta varten eikä kyseistä tietoa lähtökohtaisesti saa myöhemmin hyödyntää muulla tavalla. Saarikan tulee voida osoittaa, että kerätyt tiedot ovat virheettömiä ja henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia. Rekisteröidyllä on oikeus vaatia virheellisten tietojen korjaamista.

4.2 Tallentaminen ja säilyttäminen

Tietosuoja-asetus sallii tiedon säilyttämisen tarpeelliseksi ajaksi. Tarpeellisen ajan käsite ei ole yksiselitteinen, mutta määräämätöntä aikaa tietojen käsittelyyn ilman perustetta tai rekisteröidyn suostumusta ei ole.

Henkilötiedon elinkaari organisaatiossa päättyy, kun tiedon käyttötarkoitus tai organisaation oikeus käyttää ja hyödyntää kyseistä tietoa päättyy.

4.3 Muokkaaminen

Henkilötietojen muokkaamista ja muuttamista koskevat samat säännöt ja ohjeet kuin muutakin tietoa Saarikassa. Tietoa on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

4.4 Luovuttaminen

Saarikka käsittelee henkilötietoja ensi sijassa itse ja luovuttaa henkilötietoja ulkopuolisille pääsääntöisesti vain lakisääteisesti tai henkilön tai hänen edustajansa nimenomaisella suostumuksella. Luovutuksiin liittyvät luovutukset kuvataan Saarikan tietosuojaselosteiden kuvauksissa, jotka ovat rekisteröityjen saatavilla Saarikan verkkosivuilla osoitteessa www.saarikka.fi -> ohjeet asiakkaalle -> asiakastiedot -> tietosuojaselosteet. Saarikan tietojen luovuttamiskäytäntöjä ohjaa Saarikan tietopalveluohje.

4.5 Pseudonymisointi ja anonymisointi

Henkilötietojen suojaamiseksi tiedot voidaan pseudonymisoida tai anonymisoida.

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja.

Anonymisointi tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei voida enää tunnistaa niistä. Se, voidaanko jokin tieto lopulta katsoa anonyymiksi vai ei, edellyttää tapauskohtaista arviointia. Henkilö voi olla tunnistettavissa muutenkin kuin nimen perusteella.

4.6 Poistaminen ja arkistointi

Vanhentuneita ja tarpeettomia henkilötietoja ei tule säilyttää. Tiedot, joita ei enää tarvita, hävitetään tai siirretään arkistoon säilyttäväksi Saarikan arkistonmuodostussuunnitelman mukaisesti. Lainsäädännössä on erityissäännöksiä henkilötietojen säilyttämisajoista, joita Saarikan tulee noudattaa, mm. julkishallinnossa on erityismääräyksiä viranhaltijoiden/työntekijöiden tietojen säilyttämisestä.

5. REKISTERÖIDYN OIKEUDET

Rekisteröityjä informoidaan heidän oikeuksistaan www.saarikka.fi- sivuilla ja samalla kerrotaan myös, kuinka he voivat käyttää oikeuksiaan.

Rekisteröidyn oikeudet EU-tietosuoja-asetuksen mukaan ovat:

5.1 Oikeus saada läpinäkyvää informaatiota

Rekisteröityä on informoitava, miten hänen henkilötietojaan käsitellään. Myös sosiaali- ja terveydenhuollon tietyt erityislait säätävät informointivelvoitteesta: SoTeASL 17§, eResL 4§, AsiakasL 13§.

Tietosuojaselosteet Saarikan kotisivuilla ovat informaatioasiakirjoja, jotka on tarkoitettu antamaan tietoa henkilötietojen käsittelystä kussakin henkilörekisterissä.

Asetus asettaa määräaikoja informoinnille ja rekisteröidyn pyynnön perusteella toteutettaville toimenpiteille. Asetuksen mukaan tieto toimenpiteistä, joihin rekisteröidyn pyynnön johdosta on ryhdytty, tulee antaa ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa, jolloin pyytäjälle on kuukauden kohdalla ilmoitettava viivästymisestä sekä kerrottava viivästymisen syyt.

5.2 Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada pääsy häntä koskeviin henkilötietoihin. Jokaisella on oikeus tarkastaa henkilörekisteriin tallennetut tietonsa ja miten niitä on käsitelty. Oikeuteen sisältyy myös mahdollisuus saada kopiot esim. potilasasiakirjoista. Pyyntö osoitetaan Saarikalle rekisterinpitäjänä. Tietopyyntöihin on käytettävissä mm. Saarikan tietopyyntölomakkeet: www.saarikka.fi -> ohjeet asiakkaille -> asiakastiedot -> asiakkaan ja potilaan oikeudet rekisteritietoihin. Hakemus voi olla myös vapaamuotoinen tai se voidaan hoitaa henkilökohtaisen käynnin yhteydessä.

5.3 Oikeus tietojen oikaisemiseen ja poistamiseen

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.

Oikeutta poistaa tietoja ei sovelleta Saarikan lakisääteisissä rekistereissä.

5.4 Oikeus käsittelyn rajoittamiseen

Rekisterinpitäjänä Saarikka vastaa henkilötietojen oikeellisuudesta ja käsittelystä Järjestelmissä käsitellään ainoastaan tehtävien toteuttamisen kannalta välttämättömiä tietoja Saarikan lakisääteisten velvoitteiden täyttämiseksi, eikä rekisteröidyn asiaa voida käsitellä ilman näitä tietoja.

5.5 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu, jos

- käsittely perustuu suostumukseen tai sopimukseen ja
- käsittely suoritetaan automaattisesti.

Kun rekisteröity käyttää oikeuttaan siirtää tiedot järjestelmästä toiseen, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista. Oikeutta siirtää tiedot järjestelmästä toiseen ei sovelleta lakisääteisissä rekistereissä.

5.6 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia

Rekisteröidyllä on oikeus vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttöön sekä rekisterinpitäjän tai kolmannen oikeutetun edun toteuttamiseen. Rekisterinpitäjä ei saa enää tällöin käsitellä henkilötietoja, paitsi jos rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy. Suoramarkkinoinnissa rekisteröidyllä on oikeus, milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten.

Perusturvaliikelaitos Saarikalla on perusteltu oikeus yleisiin etuihin liittyvien tehtävien toteuttamiseksi käsitellä henkilötietoja. Näin on mm. kansanterveyden, sosiaalisen suojelun sekä terveydenhuoltopalvelujen hallinnon alalla.

Rekisteröity voi vastustaa tietojensa käsittelyä pyytämällä tätä rekisterinpitäjältä. Tietojen käsittely on kuitenkin välttämätöntä Saarikan lakisääteisten velvoitteiden täyttämiseksi, joten vastustaminen ei ole sosiaalipalveluissa/terveyspalveluissa/henkilöstöhallinnossa mahdollista.

5.7 Oikeus tehdä valitus valvontaviranomaiselle

Jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle tietosuojavaltuutetun toimistoon, jos hän katsoo, että henkilötietojen käsittelyssä rikotaan asetusta. Yhteystiedot valituksen tekoon tulee olla saatavilla.

Suomen tietosuojavaltuutetun toimiston yhteystiedot:

Käyntiosoite: Ratapihankatu 9, 6.krs, 00520 Helsinki
Postiosoite: PL 800, 00521 Helsinki
Sähköposti: tietosuoja@om.fi
Vaihde: 029 56 66700

6. REKISTERINPITÄJÄ (Saarikka)

Perusturvaliikelaitos Saarikka toimii rekisterinpitäjänä ostaessaan ja ulkoistaessaan järjestämisvastuullaan olevia palveluja. Saarikka on viimesijaisesti vastuussa henkilötietojen käsittelyn lainmukaisuudesta myös ostopalveluidensa tuottamisen osalta.

6.1 Saarikka vastaa ostopalveluiden osalta

- EU:n yleisessä tietosuoja-asetuksessa rekisterinpitäjälle säädetyistä velvoitteista
- asiakirjojen pysyvästä säilyttämisestä ja hävittämisestä
- sen varmistamisesta, että palveluntuottaja käsittelee asiakastietoja lainsäädännön ja sopimuksen mukaisesti, säännöllinen palveluntuottajan valvonta
- tietosuoja-asetuksen mukaisten henkilön oikeuksien toteuttamisesta yhdessä palveluntuottajan kanssa sekä niihin liittyvistä päätöksistä
- julkisuuslaissa viranomaiselle säädetyistä velvoitteista sekä asiakirjojen tiedonsaantiin liittyvistä päätöksistä

6.2 Saarikan velvollisuudet tietosuoja-asetuksen mukaisesti

Seloste käsittelytoimista

Saarikan on rekisterinpitäjänä ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Saarikassa on päädytty yhdistämään käsittelytoimien seloste ja informointiasiakirja rekisteröidyille. Näin ollen Saarikassa laaditaan vain tietosuojaselosteet, joihin yhdistetään käsittelytoimien selosteeseen tarvittavat tiedot:

- rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä olevat vastaanottajat
- tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
- mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat
- mahdollisuuksien mukaan yleinen kuvaus käsittelyn turvallisuuteen liittyvistä teknisistä ja organisatorisista turvatoimista.

Ilmoitusvelvollisuus tietoturvaloukkauksesta

Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä Saarikalle, jonka on ilmoitettava tietoturvaloukkauksesta mahdollisuuksien mukaan 72 tunnin kuluessa valvontaviranomaiselle.

Saarikan on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Lisäksi asiasta on ilmoitettava rekisteröidylle tietyissä tapauksissa ilman aiheetonta viivytystä.

Tietojen suojaaminen:

Rekisterinpitäjänä Saarikan on toteutettava tarpeelliset hallinnolliset ja tekniset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelemiseltä.

Tietojen suojaamiseksi tulee huolehtia, että:

- kirjauduttaessa henkilötietoa sisältäviin järjestelmiin, tulee tunnistamisessa käyttää vähintään käyttäjätunnusta ja salasanaa
- tekninen tietoturvallisuus täyttää arkaluonteisen tiedon käsittelemiseen tarvittavat minimivaatimukset (kuten palomuuri, haitallisen koodin torjunta, salausjärjestelmä, langaton yhteys)
- fyysinen turvallisuus täyttää Saarikan miminivaatimukset (kuten lukitus, hälytys, kamaravalvonta, vartiointi, toimi- ja säilytystilat)
- henkilöstö perehdytetään ja koulutetaan säännöllisesti tietosuojan perusteisiin
- teknisten ja hallinnollisten toimenpiteiden tehokkuutta testataan ja arvioidaan säännöllisesti
- häiriötilanteesta kyetään toipumaan (mm. palauttamaan nopeasti tietojen saatavuus) mahdollisimman nopeasti ja vähin vaurioin
- kyetään takaamaan tietojenkäsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus
- on tunnistettu ne työtehtävät, jotka käsittelevät työtehtäviensä vuoksi henkilötietoja
- viestintävälineitä, kuten sähköpostia, käytettäessä tiedostetaan niiden yleiset ja järjestelmäkohtaiset tietoturvapuutteet sekä käytetään niitä kompensoivia menetelmiä (esim. salattu sähköposti)

7. PALVELUNTUOTTAJA (henkilötietojen käsittelijä)

Ulkoisen palveluntuottajan eli henkilötietojen käsittelijän tulee käsitellä henkilötietoja toiminnassaan vastuullisesti ja huolellisesti Saarikan toimeksiannosta ja lukuun.

7.1 Palveluntuottaja vastaa

- asiakastietojen kirjaamisesta ja tallettamisesta palvelunjärjestäjän lukuun
- käyttöoikeuksien antamisesta asiakastietoihin omassa organisaatiossaan
- henkilötietojen käsittelyn aktiivisesta ohjauksesta ja valvonnasta organisaatiossaan

- alkuperäisten asiakirjojen toimittamisesta palvelunjärjestäjälle siten kuin on sovittu, kuitenkin viipymättä asiakassuhteen päätyttyä
- tietosuoja-asetuksessa ja julkisuuslaissa säädettyjen asiakkaan oikeuksien toteuttamisesta yhdessä palvelunjärjestäjän kanssa

7.2 Palveluntuottajan yleiset velvoitteet *(tietosuoja-asetus 28 artikla)*

Velvoitteet tulevat EU:n yleisestä tietosuoja-asetuksesta, solmittavasta sopimuksesta Saarikan kanssa sekä muusta lainsäädännöstä ja ohjeistuksista.

Tietopohjaan tutustuminen

- tietosuojalainsäädäntö
- käsitteet tutuiksi
- henkilötiedon tunnistaminen
- rekisterin pitäjyyden määräytyminen

Sopimus

- kirjallinen sopimus laaditaan Saarikan kanssa, jonka yhteyteen liitetään henkilötietojen käsittelyehdot henkilötietojen käsittelijälle
- sopimuksessa ilmoitetaan henkilötietojen käsittelijän tarvittavat yhteystiedot, mm. yhteyshenkilö
- Saarikka voi pyytää infoa henkilötietojen käsittelijältä hänen tietojen käsittelytavoistaan ennen sopimuksen allekirjoittamista
- sopimuksessa yksilöidään ja määritetään palveluntuottajan oikeudet ja velvoitteet Saarikan omistamiin aineistoihin
- sopimuksessa määritetään Saarikan oikeudet ja velvollisuudet rekisterinpitäjänä
- Huom: Yksityinen palveluntuottaja on palvelunjärjestäjä ja rekisterinpitäjä sen täysin omien, itse maksavien asiakkaiden osalta ja näiden asiakkaiden tiedot talletetaan yksityisen palvelunantajan omaan asiakasrekisteriin.

Seloste käsittelytoimista

- ohjeita selosteen laatimiseen ja valmis pohjakin löytyy linkistä https://tietosuoja.fi/henkilotietojen-kasittelijan-seloste-kasittelytoimista
- terveyden- ja sosiaalihuollon tehtävät aiheuttavat korkean riskin yksilön oikeuksille, niihin liittyviin tehtäviin selosteen tulee olla Saarikassa saatavilla
- dokumentaatiokuvaus tarvitaan tietosuoja-asetuksen vaatimusten toteutustavoista myös mahdollisilta alihankkijoilta (salassapitosopimukset, käyttäjärajoitukset, koulutus, tekninen tietoturva jne.)
- käsittelytoimien kuvaukset laitetaan laadittavan sopimuksen liitteiksi Saarikan asiankäsittelyjärjestelmään

Sitoutuminen

- sopimukseen, ohjeisiin ja henkilötietojen käsittelyn periaatteisiin
- salassapitoon, tietojen hyväksikäyttökieltoon ja vaitiolovelvollisuuden toteuttamiseen
- tietosuojasta ja tietoturvasta annettuihin sääntöihin

Palveluntuottaja on vastuussa asiakirja-aineistosta siihen saakka, kunnes luovuttaminen ohjeistetusti Saarikalle on tapahtunut

Salassapito/vaitiolovelvoitteet

- palveluntuottaja on vastuussa oman henkilöstönsä luotettavuudesta
- palveluntuottajan on huomioitava käyttöoikeuksia myöntäessään, että tietoja käsittelevät vain siihen oikeutetut henkilöt työtehtäviensä mukaisesti
- henkilöstön on allekirjoitettava salassapitosopimus työsuhteen alkaessa; salassapito koskee myös palvelua/työsuhdetta, joka on jo päättynyt
- ulkopuolisten pääsy Saarikan henkilötietoihin on estettävä käsittelyn joka vaiheessa
- henkilötietojen käsittelyn aktiivinen ohjaus ja valvonta on toteutettava palveluntuottajan omassa organisaatiossa

Tietoturva/tietosuoja/suojaamisvelvoite

- mahdolliset riskit palveluntuottajan henkilötietojen käsittelyssä on huomioitava; tietosuoja-asetus korostaa riskienhallintaa ja arviointia
- palveluntuottajan on sitouduttava sopimuksessa toteuttamaan ja dokumentoimaan riittävät turvatoimet henkilötietojen suojaamiseksi
- henkilörekisterit on suojattava riittävästi: mm. tietokoneiden virustorjunta ja palomuurit, toimitilojen kulunvalvonta, riittävät ja asiantuntevat resurssit, henkilöstön kouluttaminen, omavalvonnan kautta tapahtuva käytönvalvonta
- lokitietojen keräämiseen palveluntuottajan tietojärjestelmästä on oltava mahdollisuus
- tarvittaessa palveluntuottajan on nimettävä toimintaansa tietosuojavastaava, ainakin jos tuotettavassa palvelussa käsitellään arkaluontoista, salassa pidettävää tietoa

Saarikka on velvollinen valvomaan palveluntuottajan tietoturvatoimien täytäntöönpanoa säännöllisten **tarkastusten** avulla.

Ilmoitusvelvollisuus

- **ongelmatilanteissa** on reagoitava nopeasti

- palveluntuottajalla on välitön, **kirjallinen** ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksesta Saarikalle: ilmoitus tehdään kyseisen palvelualueen johtajalle tai Saarikan tietosuojavastaavalle -> Saarikan tulee ilmoittaa tietoturvaloukkaukset 72 tunnin sisällä valvontaviranomaiselle (Tietosuojavaltuutetun toimisto)

- Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi

    - hävinnyt tiedonsiirtoväline, kuten USB-tikku, joka sisältää henkilötietoja
    - varastettu tai kadonnut laite: tietokone/älypuhelin
    - ulkopuolinen henkilö lukee tietoja auki jääneeltä tietokoneelta
    - hakkerointi
    - haittaohjelmatartunta
    - kyberhyökkäys
    - tulipalo datakeskuksessa

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

- Lisätietoa tietoturvaloukkauksen ilmoittamisesta saa mm. tietosuojavaltuutetun toimiston nettisivuilta:
  https://tietosuoja.fi/tietoturvaloukkaukset
  Loukkaukseen liittyvät tiedot tulee ilmoittaa mahdollisimman tarkasti.

Käsittelijän omat alihankkijat

- palveluntuottajalla on vastuu alihankkijastaan, jos tämä ei täytä tietosuojavelvoitteitaan
- Saarikan on tiedettävä ja hyväksyttävä mahdolliset palveluntuottajan alihankkijat (sopimusasia)
- Saarikan aineiston siirtoon (esim. pilvipalveluun) tarvitaan aina Saarikan lupa

Avustamisvelvollisuus

- palveluntuottaja on velvollinen avustamaan Saarikkaa teknisillä ja organisatorisilla toimenpiteillä ja tiedoksi saattamalla, että sen henkilötietojen käsittely on mahdollisimman turvallista ja käsittelyyn kohdistuvat riskit ovat hallinnassa
- rekisteröityjen oikeuksien tulee toteutua asetuksen mukaisesti ja heidän oikeuksiaan tulee kunnioittaa palveluntuottajan tehtävissä
- palveluntuottaja avustaa Saarikkaa tietopalvelutehtävissä aina tarvittaessa

Yksilöillä on lukuisia oikeuksia, kuten oikeus saada pääsy itseään koskeviin henkilötietoihin ja saada virheelliset tiedot oikaistuiksi. Tietopyynnöt ohjeistetaan lähettämään Saarikalle, joka rekisterinpitäjänä ja viranomaisena vastaa tietopalvelun asianmukaisuudesta ja päättää tiedon luovuttamisesta.

Käytettävissä ovat mm. Saarikan tietopyyntölomakkeet, jotka löytyvät www.saarikka.fi -> ohjeet asiakkaalle -> asiakastiedot-> asiakkaan ja potilaan oikeudet rekisteritietoihin.

Toiminnan dokumentointi

- palveluntuottajan on ylläpidettävä omavalvontasuunnitelmaa, jos siihen on velvoite
- tietosuoja-asetuksen mukainen osoitusvelvollisuus asetuksen noudattamisesta koskee myös palveluntuottajaa henkilötietojen käsittelijänä
- toiminnassa tapahtuvat muutokset informoidaan Saarikalle välittömästi

Asiakaskohtainen dokumentointi

- asiakasta koskevien tietojen on oltava todennettavissa myöhemmin, tietojen tulee säilyä turvallisesti
- asiamukaiset merkinnät kaikesta henkilön hoitoon liittyvästä (ei käsin kirjattuja vihkoja)
- Saarikan tietojärjestelmien mahdollisesta yhteiskäytöstä ja käyttöoikeuksista on laadittava sopimus

Auditointioikeus

- velvoite sallia ja osallistua Saarikan tai muun sen valtuuttaman auditoijan suorittamaan auditointiin

Vahingonkorvausvastuu

- Saarikalla on viimekäden vastuu henkilötietojen käsittelyn lainmukaisuudesta, joten Saarikka vastaa myös yhteistyökumppaniensa toimista
- asetuksen myötä vahingonkorvauskanne voi kohdistua myös suoraan palveluntuottajaan /henkilötietojen käsittelijään, joka voi joutua vastuuseen aiheutuneista vahingoista
- sanktiot sovitaan sopimuksessa palveluntuottajan ja Saarikan välillä

Tietojen poistaminen/palauttaminen Saarikalle

- ostopalvelun päätyttyä alkuperäiset henkilötiedot palautetaan Saarikalle sovitusti, jollei lakivelvoitetta niiden säilyttämiseen palveluntuottajalla ole (mm. yksityiset terveydenhuollon palveluntarjoajat)
- jäljennökset on tuhottava huolellisesti; henkilötietoja ei laiteta yleisiin roskiin
- luovutuksen jälkeen vastuu asiakirjoista siirtyy palveluntuottajalta Saarikalle
- tarkempi ohjeistus löytyy Saarikan asiakirjojen käsittelyohjeesta ulkopuolisille palveluntuottajille

Mitä velvoitteiden noudattamatta jättämisestä voi seurata?

- tietosuojaviranomaisen huomautus
- määräys käsittelytoimien saattamisesta tietosuoja-asetuksen mukaiseksi
- käsittelylle väliaikainen tai pysyvä kielto
- hallinnollinen sakko
- kts. https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Ohjeita

Ylin tietosuojaviranomainen on Tietosuojavaltuutetun toimisto: www.tietosuoja.fi. Tietosuoja-aiheista koulutusta saa esimerkiksi osoitteesta arjentietosuoja.fi löytyviltä videoilta. Samalla sivustolla voi tehdä myös tietosuoja-aiheisen testin.

8. KESKEINEN TERMINOLOGIA

Henkilötieto
Kaikenlaiset luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi (kuten nimi, henkilötunnus, osoite, verkkotunnistetieto tai yhden tai useamman hänelle tavanomaisen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä)

Henkilötietojen käsittelijä
Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muut taho, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta (kuten ostopalvelu- tai palvelusetelituottaja)

Henkilötietojen käsittely
Henkilötietoon sen elinkaaren aikana kohdistuvat automaattiset tai manuaaliset toimenpiteet kuten kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen, hakeminen, luovuttaminen (siirtämällä, levittämällä, asettamalla saataville), yhdistäminen, poistaminen, tuhoaminen, salakirjoittaminen, arkistointi.

Henkilörekisteri
Mikä tahansa jäsenneltyä henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Henkilörekisteri voi olla keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Käyttötarkoitussidonnaisuus
Henkilötietojen käsittelyn tulee tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin tarkoitukseen, jolla ei ole sidonnaisuutta kerättyyn käyttötarkoitukseen. Käyttötarkoitussidonnaisuutta ei kuitenkaan tarvitse olla arkistointitarkoitusta, historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

Läpinäkyvyys
Rekisteröidylle tulisi olla läpinäkyvää, miten häntä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään tai on aikeissa käsitellä. Läpinäkyvyyden periaatteen mukaisesti henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä.

Rekisterinpitäjä
Organisaatio (kuten kunta tai sen palveluntuottaja), jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Rekisteröity
Luonnollinen henkilö, jonka henkilötiedoista on kyse.

9. HENKILÖTIETOJEN KÄSITTELYÄ OHJAAVIA LAKEJA, ASETUKSIA ja SUOSITUKSIA

TUTUSTU LAKEIHIN; JOITA SOVELLETAAN TEHTÄVÄÄN!

Tärkeimmät lait: www.finlex.fi

- EU:n yleinen tietosuoja-asetus (2016/679)
- Tietosuojalaki (1050/2018)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Hallintolaki (434/2003)
- Kuntalaki (410/2015)
- Arkistolaki (831/1994)
- Työsopimuslaki (55/2001)
- Kirjanpitolaki (1336/1997)
- Saarikan voimassa oleva hallintosääntö
- Suomen kuntaliiton suositukset
- Laki potilaan asemasta ja oikeuksista (785/1992)
- STM:n asetus potilasasiakirjoista (298/2009)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sosiaalihuollon asiakasasiakirjoista (254/2015)
- Laki sosiaalihuollon ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), uudistuu HE 300/2018
- Muu sosiaali- ja terveydenhuollon erityislainsäädäntö