

## Kanervakoti

### Tietoturvan omavalvontasuunnitelma

#### Sisällys

Tietosuoja asiakastietojen käsittelyssä.....	1
Keskeiset lait.....	1
Henkilötietojen käsittelyn ehdot .....	2
Tietosuojaselosteet.....	9
Asiakkaan oikeus tarkastaa rekisteritietonsa sekä lokirekisterimerkinnot .....	9
Tietoturva asiakastietojen käsittelyssä .....	14
Määritelmä ja sisältö .....	14
Organisaation henkilöstö, käyttöoikeudet sekä tilat ja laitteet vaatimukset .....	15
Henkilöstön salassapito ja -tietoturvasitoumus .....	16
Tietoturvan omavalvontasuunnitelman allekirjoitus .....	17

## Tietoturvan omavalvontasuunnitelma

Tässä dokumentissa on kuvattu sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 19 h §:n mukainen tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä omavalvontasuunnitelma.

### Tietosuoja asiakastietojen käsittelyssä

#### Keskeiset lait

Sosiaali- ja terveystieteissä käsiteltävät potilas- ja asiakastiedot ovat henkilötietolain (523/1999) tarkoittamia henkilötietoja. Siten potilas- ja asiakastietojen käytössä ja käsittelyssä noudatetaan henkilötietolain säännöksiä sekä yksityisen että julkisen sektorin toiminnassa.

Asiakasasiakirjat, jotka sisältävät tietoa henkilön terveydentilasta tai hänen saamastaan terveydenhuollon, kuntoutuksen tai sosiaalihuollon palvelusta ovat salassa pidettäviä ja niihin liittyvien asiakastietojen käsittely ja säilyttäminen on toteutettava siten, että asiakkaan tietosuoja ja tietoturva toteutuvat.

Julkisuuslain mukaan jo tieto sosiaali- ja terveystoimen asiakkuudesta on salassa pidettävä tieto (24§ 25-kohta)

KANERVAKOTI - Kanervahemmet ry

Y-tunnus: 0221424-9

ANKKURISAARENTIE 4-6

Puh: 050 5692873

02160 ESPOO

toiminnanjohtaja@kanervakoti.fi

Henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomais määräyksiä ja 25.5.2018 alkaen EU:n yleistä tietosuojasetusta.

Sosiaalipalveluja annettaessa asiakkaiden tiedoista muodostuu henkilörekisteri tai -rekistereitä (henkilötietolaki 10 §), tästä syntyy myös velvoite informoida asiakkaita henkilötietojen tulevasta käsittelystä sekä rekisteröidyn oikeuksista.

Asiakkaista laadittavat asiakirjat tai heistä kerättävät tiedot määritellään toimeksianto- tai palvelusopimuksessa.

### **Potilas- ja asiakastietojen käsittelyssä huomioitavia lakeja:**

Henkilötietolaki 523/1999

Laki potilaan asemasta ja oikeuksista 785/1992

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 812/2000

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007

### **Potilas- ja asiakastietojen käsittelyssä huomioitavia säädöksiä:**

Henkilörekisterin tietojen tarkastaminen (Hyvä tietää -sarja 1/2005)

Henkilörekisteriin talletettujen tietojen korjaaminen (Hyvä tietää -sarja 2/2005)

Henkilötietojen käsittely suostumuksen perusteella (Hyvä tietää -sarja 2/2001)

Malli julkisen terveydenhuollon potilaiden informoinnista (Mallit-sarja 3/2000)

Sosiaalihuollon asiakkaiden informointi (Mallit-sarja 1/2000)

Henkilötietolain mukainen yleinen informointivelvollisuus (Asiaa tietosuojasta -sarja 2/1999)

**Tietosuojalla** tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käsittelemiseltä. Tietosuojaan kuuluvat näin ollen yksityisten henkilöiden yksityisyyden suoja sekä sitä turvaavat oikeudet ja edut henkilötietoja käsiteltäessä.

### **Henkilötietojen käsittelyn ehdot**

Kanervakoti (myöhemmin "Käsittelijä") käsittelee kaikkia asiakastietoja siten kun on sovittu Espoon kaupungin (myöhemmin "Rekisterinpitäjä") kanssa 30.12.2019 allekirjoitetun Ikääntyneiden tehostetun palveluasumisen hankinta 5450/2018 " sopimuksen ml. liitteen 1 Henkilötietojen käsittelyn ehdot (myöhemmin "Sopimus") mukaan sekä vastaavalla tavalla, kun on kyse muusta kun ko sopimuksen mukaisesta rekisterinpitäjästä.

## **Yleistä**

Tässä tietoturvan omavalvontasuunnitelmassa kuvataan, miten Käsittelijän Rekisterinpitäjän toimeksiannosta käsittelee henkilötietoja Rekisterinpitäjän puolesta ja lukuun.

”Rekisterinpitäjän henkilötiedoilla” tarkoitetaan näissä ehdoissa henkilötietoja, joista Rekisterinpitäjä vastaa.

”Sopimuksella” tarkoitetaan näissä ehdoissa Rekisterinpitäjän ja Käsittelijän välillä tehtyä sopimusta, jonka perusteella henkilötietoja käsitellään, sekä muutossopimusta, jolla muutetaan edellä tarkoitettu sopimus vastaamaan EU:n yleistä tietosuoja-asetusta.

Osapuolet noudattavat toiminnassaan kulloinkin voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomais määräyksiä ja 25.5.2018 alkaen EU:n yleistä tietosuoja-asetusta.

Sopimusta tehtäessä tietosuojaa koskeva lainsäädäntö on muutostilassa. Osapuolet tarkistavat Sopimusta tarvittaessa, jos lainsäädäntöön tai sen tulkintaa koskeviin suosituksiin, ohjeistuksiin tai määräyksiin tulee muutoksia.

## **Osapuolten roolit henkilötietojen käsittelyssä**

Rekisterinpitäjä toimii henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön tarkoittamana rekisterinpitäjänä silloin, kun se määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Ryhmittymän ollessa Käsittelijänä tämän sopimusliitteen velvoitteet koskevat kaikkia ryhmittymän jäseniä, ja ryhmittymän käyttämiä alihankkijoita, jotka osallistuvat henkilötietojen käsittelyyn.

Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä Rekisterinpitäjän ja Käsittelijän velvollisuudet ja oikeudet kuvataan Sopimuksen liitteenä olevassa ”käsittelytoimien kuvauksessa” ja/tai muussa Rekisterinpitäjän kirjallisessa ohjeistuksessa. Jos käsittelytoimien kuvausta ja/tai muuta kirjallista ohjeistusta ei ole tehty tai se on puutteellinen, Rekisterinpitäjä laatii tai täydentää käsittelytoimien kuvausta tarvittaessa yhteistyössä Käsittelijän kanssa. Käsittelijän on ilmoitettava Rekisterinpitäjälle, jos tämän antama käsittelytoimien kuvaus tai muu ohjeistus on puutteellinen tai, jos Käsittelijä epäilee sitä lainvastaiseksi.

## **Käsittelijän velvollisuudet**

## Henkilötietojen käsittely

Käsittelijä vastaa siitä, että palvelu on kulloinkin voimassa olevan henkilötietolainsäädännön ja Sopimuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä on säädetty sisäänrakennetusta ja oletusarvoisesta tietosuojasta sekä hyvästä tietojen käsittelytavasta.

Jos Sopimuksen perusteella laaditaan tai käsitellään potilasasiakirjoja tai asiakasasiakirjoja, Käsittelijä sitoutuu laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjoja ja asiakasasiakirjoja koskeva lainsäädäntö ja viranomais määräykset edellyttävät.

Käsittelijän tulee noudattaa Sopimuksen mukaisessa toiminnassa lakia viranomaisten toiminnan julkisuudesta (621/1999) sekä muita salassapidosta ja vaitiolovelvollisuudesta annettuja voimassa olevia säädöksiä.

Käsittelijän Sopimuksen mukaisessa toiminnassa syntyvät asiakkuutta koskevat asiakirjat ovat Rekisterinpitäjän asiakirjoja. Toiminnassa syntyvien asiakirjojen käsittelyyn ja arkistointiin noudatetaan samoja periaatteita kuin muihinkin viranomaisten asiakirjoihin.

Käsittelijä saa käyttää henkilötietoja vain Sopimuksen mukaisten palvelujen toteuttamiseen ja silloinkin ainoastaan Sopimuksen tarkoituksen edellyttämässä laajuudessa ja vain sinä aikana, kuin se on Sopimuksen kohteen täyttämiseksi välttämätöntä.

Käsittelijän on käsiteltävä henkilötietoja Rekisterinpitäjän antaman ohjeistuksen ja niiden päivitysten mukaisesti. Henkilötietoja ei saa käyttää esimerkiksi mainontaan tai markkinointiin eikä niitä saa ilman Rekisterinpitäjän lupaa luovuttaa ulkopuolisille. Käsittelijän on säilytettävä henkilötietoja niin, että ne eivät joudu sivullisten käsiin.

Sen lisäksi, mitä muualla Sopimuksessa on sovittu henkilötietojen suoja, tietoturvallisuutta ja tietojen salassapitoa koskevista vaatimuksista, Käsittelijä sitoutuu toteuttamaan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn turvallisuuden varmistamiseksi ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Käsittelijä huolehtii Sopimuksen perusteella käsittelemiensä henkilötietojen asianmukaisesta suojaamisesta omien käytäntöjensä, Sopimuksen vaatimusten ja

Rekisterinpitäjän käsittelytoimien kuvauksen ja/tai kirjallisen ohjeistuksen mukaisesti varmistaakseen henkilötietojen luottamuksellisuuden, eheyden ja saatavuuden.

Käsittelijän on huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan automaattisesti irrottaa järjestelmästä siirrettäväksi toiseen järjestelmään, silloin kun se on teknisesti mahdollista. Jos osapuolet ovat sopineet Rekisterinpitäjän aineiston tallentamisesta Käsittelijän hallinnassa olevaan järjestelmään tai laitteeseen, Käsittelijä huolehtii siitä, että Rekisterinpitäjän aineisto pystytään palauttamaan järjestelmän tai laitteen vikatilanteessa.

Käsittelijällä on oltava valmius asettaa ja hallinnoida tietojen luovutuksia koskevia rajoituksia, jollaisia voi aiheutua esimerkiksi väestötietolain mukaisesta rekisteröidyn turvakiellosta. Käsittelijän tulee pystyä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan Rekisterinpitäjän vaatimalla tavalla. Rekisteröidyn henkilötietojen rajoittaminen ei saa johtaa muiden rekisterissä olevien henkilötietojen rajoittamiseen, ellei Rekisterinpitäjän ja Käsittelijän kesken kirjallisesti toisin sovita.

Käsittelijä korjaa viipymättä havaitut henkilötietojen käsittelyä koskevat virheet tai puutteet.

Käsittelijä dokumentoi sovitut ja toteutetut toimenpiteet ja huolehtii siitä, että dokumentaatio on ajan tasalla. Osapuolet arvioivat teknisiä ja organisatorisia toimenpiteitä ja niiden riittävyyttä säännöllisesti.

Käsittelijä käsittelee henkilötietoja Sopimuksen ja Rekisterinpitäjän antamien kirjallisten ohjeiden mukaisesti.

Käsittelijä ilmoittaa ilman aiheetonta viivytystä Rekisterinpitäjälle, jos Rekisterinpitäjän antamat ohjeet tai Käsittelijän sisäiset ohjeet ovat puutteellisia tai jos Käsittelijä epäilee niitä lainvastaisiksi.

Rekisterinpitäjällä on oikeus muuttaa, täydentää ja päivittää Käsittelijälle antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Käsittelijä tekee tarvittavat muutostyöt Rekisterinpitäjän ohjeiden mukaisesti. Käsittelijä ja muut henkilötietojen käsittelijät sitoutuvat noudattamaan näitä muutettuja, täydennettyjä tai päivitettyjä ohjeita.

### **Käsittelijän tietosuojavastaava**

Käsittelijä on velvollinen nimeämään tietosuojasta vastaavan yhteyshenkilön henkilötietojen käsittelyä varten. Käsittelijä ilmoittaa kirjallisesti tässä kohdassa tarkoitetun yhteyshenkilön tai tietosuojavastaavan yhteystiedot ja niiden muutokset Rekisterinpitäjälle.

Käsittelijän tietosuojavastaava tai muu tietosuojasta vastaava yhteyshenkilö

Yrityksen nimi	KANERVAKOTI-Kanervahemmet ry
Y-tunnus	0221424-9
Osoite	ANKKURISAARENTIE 4-6 02160 ESPOO
Tietosuojavastaavan nimi ja titteli	Tarja Kiesi, toiminnanjohtaja
Puhelinnumero	050 5692873
Sähköpostiosoite	toiminnanjohtaja@kanervakoti.fi

### Käsittelijän henkilöstö

Käsittelijä huolehtii siitä, että henkilötietoja käsittelevät vain ne Käsittelijän lukuun työskentelevät henkilöt, joiden työtehtäviin Rekisterinpitäjän aineiston käsittely kuuluu. Käsittelijän on varmistettava, että jokainen Käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy Rekisterinpitäjän henkilötietoihin, on tietoinen henkilötietojen käsittelyyn liittyvistä velvoitteistaan ja käsittelee niitä ainoastaan Sopimuksen ja osapuolten ohjeiden mukaisesti.

Käsittelijä varmistaa, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee lakisääteinen salassapitovelvollisuus. Käsittelijän tulee ohjeistaa henkilöstönsä salassapitoa koskevista säännöksistä ja menettelyistä.

### Käsittelijän avustamis- ja tiedonantovelvollisuus

Käsittelijä saattaa Rekisterinpitäjän saataville tämän pyynnöstä kaikki tiedot, jotka Rekisterinpitäjä tarvitsee rekisterinpitäjälle ja käsittelijälle säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja osallistuu pyydettyä sovittulla tavalla Rekisterinpitäjän vastuulla olevien kuvausten ja muiden dokumenttien, kuten EU:n yleisen tietosuojasetuksen mukaisen vaikutustenarvioinnin, laatimiseen ja tekemiseen sekä ennakkokuulemisen suorittamiseen ja mahdollisen tietosuojaa koskevan sertifiointin hankkimiseen.

Käsittelijä sallii Rekisterinpitäjän tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin.

Ellei Sopimuksen mukaisista palvelutasovaatimuksista muuta johdu, Käsittelijä sitoutuu reagoimaan viimeistään 72 tunnin kuluessa Rekisterinpitäjän yhteydenotosta ja vastaamaan viimeistään yhden (1) viikon kuluessa

KANERVAKOTI - Kanervahemmet ry  
ANKKURISAARENTIE 4-6  
02160 ESPOO

Y-tunnus: 0221424-9  
Puh: 050 5692873  
toiminnanjohtaja@kanervakoti.fi

Rekisterinpitäjän tietosuojaa koskeviin palvelupyyntöihin tai reklamaatioihin tai muihin viesteihin, pois lukien EU:n yleisen tietosuoja-asetuksen mukaiset tietoturvaloukkaukset, joihin sovelletaan Sopimuksessa määritettyjä määräaikoja.

## **Rekisteröityjen pyynnöt**

Käsittelijä ilmoittaa viipymättä Rekisterinpitäjälle kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn voimassa olevan lainsäädännön mukaisten oikeuksien käyttämistä. Käsittelijä ohjaa kolmansien osapuolten tekemät Rekisterinpitäjän aineistoa koskevat tietopyynnöt ilman aiheutonta viivytystä Rekisterinpitäjälle siltä osin, kuin Käsittelijällä ei ole lainsäädäntöön perustuvaa velvollisuutta vastata tietopyyntöihin.

Käsittelijä avustaa Rekisterinpitäjää, jotta Rekisterinpitäjä pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyyntöt voivat edellyttää Käsittelijältä esimerkiksi avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen.

Ellei toisin sovita, Käsittelijä on velvollinen ylläpitämään luettelo rekisteröityjen henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista. Luettelo on luovutettava pyydettäessä Rekisterinpitäjälle.

## **Alihankkijat, jotka käsittelevät henkilötietoja**

Siltä osin kuin Käsittelijä käyttää toiminnassaan alihankkijoita, jotka käsittelevät henkilötietoja, alihankintaan sovelletaan Sopimuksessa kuvattuja ehtoja. Käsittelijä vastaa käyttämiensä alihankkijoiden osuudesta kuin omastaan.

Jos Käsittelijän alihankkija käsittelee Rekisterinpitäjän henkilötietoja eikä alihankkijan käyttämisestä ole sovittu Sopimuksessa, alihankkijan käyttäminen edellyttää Rekisterinpitäjän ennakkoon kirjallisesti antamaa lupaa.

Käsittelijän on ilmoitettava Rekisterinpitäjälle kirjallisesti kaikki toiminnassa käyttämänsä alihankkijat.

Käsittelijän on ilmoitettava Rekisterinpitäjälle etukäteen kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat henkilötietojen käsittelijöinä toimivien alihankkijoiden lisäämistä tai vaihtamista, ja annettava Rekisterinpitäjälle mahdollisuus vastustaa ehdotettuja muutoksia. Ilmoituksessa tulee kuvata, miten alihankkija käsittelee Rekisterinpitäjän henkilötietoja tietosuojalainsäädännön mukaisesti.

KANERVAKOTI - Kanervahemmet ry  
ANKKURISAARENTIE 4-6  
02160 ESPOO

Y-tunnus: 0221424-9  
Puh: 050 5692873  
[toiminnanjohtaja@kanervakoti.fi](mailto:toiminnanjohtaja@kanervakoti.fi)

Käsittelijän alihankkijat, jotka henkilötietojen käsittelijöinä käsittelevät Rekisterinpitäjän henkilötietoja Rekisterinpitäjän puolesta ja lukuun, sitoutuvat noudattamaan Sopimuksessa kuvattuja henkilötietojen käsittelijää koskevia velvollisuuksia sekä Rekisterinpitäjän antamia kulloinkin voimassa olevia henkilötietojen käsittelyyn liittyviä ohjeita. Käsittelijällä on velvollisuus kirjallisilla sopimuksilla sitouttaa käyttämänsä alihankkijat noudattamaan Sopimuksen ehtoja. Käsittelijä varmistaa, että Rekisterinpitäjän Sopimuksen mukainen tarkastusoikeus voidaan ulottaa alihankkijaan.

Jos Käsittelijän alihankkijat käsittelevät Rekisterinpitäjän henkilötietoja ja rikkovat tai laiminlyövät Sopimuksen tai sovellettavan lainsäädännön määräyksiä, Käsittelijä vastaa näistä rikkomisista tai laiminlyönneistä kuin omistaan. Jos Rekisterinpitäjä perustellusti katsoo, että Käsittelijän alihankkija ei täytä tietosuojavelvoitteitaan, Rekisterinpitäjällä on oikeus vaatia Käsittelijää vaihtamaan alihankkijaa.

### **Palvelun sijainti**

Ellei palvelun tuottamispaikasta ole toisin sovittu, Käsittelijällä on oikeus käsitellä Rekisterinpitäjän henkilötietoja ainoastaan Euroopan talousalueella. Henkilötietojen käsittelyllä tarkoitetaan myös pääsyn mahdollistamista Rekisterinpitäjän henkilötietoihin, esimerkiksi hallinta- ja valvontayhteyden välityksellä.

Jos osapuolet sopivat, että Käsittelijä saa siirtää Rekisterinpitäjän henkilötietoja Euroopan talousalueen ulkopuolelle, osapuolet huolehtivat siitä, että henkilötietojen siirto toteutetaan lainsäädännön mukaisesti asianmukaisella siirtosopimuksella noudattaen EU-komission kulloinkin voimassa olevia mallilausekkeita ja/tai muita tuolloin voimassa olevia henkilötietojen siirtoa koskevia vaatimuksia.

### **Tietoturvaloukkaukset**

Osapuolilla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen.

Käsittelijän on ilmoitettava välittömästi Rekisterinpitäjälle tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta tai vastattava välittömästi Rekisterinpitäjän tietoturvaloukkausta koskevaan yhteydenottoon. Lisäksi Käsittelijän on vastattava kirjallisesti Rekisterinpitäjälle ilman aiheetonta viivytystä ja viimeistään 36 tunnin kuluessa tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta tai rekisterinpitäjän tietoturvaloukkausta koskevasta yhteydenotosta. Lisäksi Käsittelijä sitoutuu ilmoittamaan Rekisterinpitäjälle ilman aiheetonta viivytystä muista palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.

Käsittelijän on annettava Rekisterinpitäjälle vähintään seuraavat tiedot tietoturvaloukkauksesta:



- 1) kuvattava tapahtunut henkilötietojen tietoturvaloukkaus, mukaan lukien asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät, sillä tarkkuudella, kuin nämä ovat tiedossa;
- 2) ilmoitettava tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;
- 3) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset; sekä
- 4) kuvattava toimenpiteet, joita Käsittelijä ehdottaa tai joita se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Henkilötietojen tietoturvaloukkauksen havaittuaan Käsittelijä ryhtyy viipymättä toimenpiteisiin tietoturvaloukkauksen vaikutusten rajoittamiseksi ja korjaamiseksi.

### **Henkilötietojen käsittelyn päättymisen**

Sopimuksen voimassaoloaikana Käsittelijä ei saa poistaa Rekisterinpitäjän lukuun käsittelemiään henkilötietoja ilman Rekisterinpitäjän nimenomaista pyyntöä.

Palveluiden toimittamisen tai asiakkaan asiakkuuden päätyttyä Käsittelijä sitoutuu palauttamaan tietoturvallisesti kaikki Rekisterinpitäjän henkilötiedot Rekisterinpitäjälle sekä poistamaan mahdolliset olemassa olevat kopiot. Käsittelijä sitoutuu palauttamisen sijasta poistamaan Rekisterinpitäjän henkilötiedot, jos Rekisterinpitäjä sitä nimenomaisesti pyytää. Henkilötietoja ei saa poistaa, jos lainsäädännössä tai viranomais määräyksissä edellytetään, että Käsittelijä säilyttää henkilötiedot.

Toiminnassa syntyvien asiakirjojen arkistoinnissa noudatetaan samoja periaatteita kuin muidenkin viranomaisten asiakirjojen arkistoinnissa.

### **Tietosuojaselosteet**

Kanervakodin tietosuojaselosteet sisältävät Henkilötietolain 523/1999 mukaiset tiedot siitä, mitä, missä ja miten Kanervakodissa asukkaiden ja henkilökunnan henkilötietoja käsitellään ja suojataan. Tietosuojaselosteet ovat luettavissa [www.kanervakoti.fi](http://www.kanervakoti.fi)

Tietosuojaseloste\_asukkaat  
Tietosuojaseloste\_henkilökunta

### **Asiakkaan oikeus tarkastaa rekisteritietonsa sekä lokirekisterimerkinnot**

Henkilörekisteriin merkityillä on henkilötietolain 26 §:n perusteella kerran vuodessa oikeus maksutta saada tietää, mitä tietoja hänestä on talletettu henkilörekisteriin.

KANERVAKOTI - Kanervahemmet ry

ANKKURISAARENTIE 4-6

02160 ESPOO

Y-tunnus: 0221424-9

Puh: 050 5692873

toiminnanjohtaja@kanervakoti.fi

Henkilörekisteriin merkityn on esitettävä pyyntö omakätisesti allekirjoitetulla asiakirjalla tai vastaavasti varmennetulla tai henkilökohtaisesti. Tiedot tulee antaa ilman aiheetonta viivytystä.

Sähköisen järjestelmän tietojen luovutuksessa syntyy luovutuksen yhteydessä lokitietoja. Ne tallennetaan luovutuslokirekisteriin, johon tallentuu tiedot luovutetuista asiakastiedoista, palvelun antajaa koskevista tiedoista, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta ja luovutusajankohdasta. Lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä nojalla asiakkaalla on oikeus saada viivytyksettä lokirekisteritiedot asiakastietojensa käsittelystä.

Asiakkaan halutessa tarkastaa rekisteri- tai lokirekisteritietonsa Espoon kaupungilta, hänen tulee täyttää pyyntöä koskeva Espoon kaupungin lomake (rekisteritietojen tarkastuspyyntölomake tai lokirekisterin tarkastuspyyntölomake, liitteenä), joka tulee osoittaa osoitteeseen: Espoon kaupunki pitkäaikaishoito/asumispalvelut, PL 2400, 02070 Espoon kaupunki.

#### **Potilas- ja asiakastietojen käsittelyssä huomioitavia lakeja:**

Henkilötietolaki 523/1999

Laki potilaan asemasta ja oikeuksista 785/1992

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 812/2000

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007

#### **Potilas- ja asiakastietojen käsittelyssä huomioitavia säädöksiä:**

Henkilörekisterin tietojen tarkastaminen (Hyvä tietää -sarja 1/2005)

Henkilörekisterin talletettujen tietojen korjaaminen (Hyvä tietää -sarja 2/2005)

Henkilötietojen käsittely suostumuksen perusteella (Hyvä tietää -sarja 2/2001)

Malli julkisen terveydenhuollon potilaiden informoinnista (Mallit-sarja 3/2000)

Sosiaalihuollon asiakkaiden informointi (Mallit-sarja 1/2000)

Henkilötietolain mukainen yleinen informointivelvollisuus (Asiaa tietosuojasta -sarja 2/1999)

**Rekisterinpitäjän nimi: Espoon kaupunki**

**Sosiaali- ja terveystoimen toimiala**

Toimittakaa tulostettu ja  
allekirjoitettu lomake osoitteeseen:  
Espoon sosiaali- ja terveystoimi  
Tietosuojavastaava  
PL 205  
02070 Espoon kaupunki

KANERVAKOTI - Kanervahemmet ry  
ANKKURISAARENTIE 4-6  
02160 ESPOO

Y-tunnus: 0221424-9  
Puh: 050 5692873  
toiminnanjohtaja@kanervakoti.fi

Asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten sosiaalihuollon ja terveydenhuollon palvelujen antajalta kirjallisesta pyynnöstä viivytyksettä lokirekisterin perusteella maksutta tietoa siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste. Asiakkaalla ei kuitenkaan ole oikeutta saada lokitietoja henkilötietolain 27 §:n 1 momentin 1-4 kohdassa tarkoitetuissa tapauksissa. Asiakas ei saa käyttää tai luovuttaa saamiaan lokitietoja edelleen muuhun tarkoitukseen. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) 18 §)



<b>Rekisterin nimi</b>	
<b>Vaatus</b>	Pyydän henkilötietolain 26 §:n perusteella saada tietää, mitä tietoja minusta on talletettu edellä mainittuun ylläpitämääne rekisteriin.
	<input type="checkbox"/> Haluan alla luetellut asiakirjat/tiedot:  <input type="checkbox"/> Haluan tarkastaa tiedot ajanjaksolta :
<b>Tarkastuspyynnön esittäjän yhteystiedot</b>	Nimi: _____ Henkilötunnus: _____ Osoite: _____ Postinumero ja –toimipaikka: _____ Puhelin: _____
<b>Päiväys ja allekirjoitus</b>	

Tarkastuspyyntö vastaanotettu, päivämäärä:  
**toimenpiteet**

**Rekisterinpitäjän**  
**HetiL 26 §)**

Tarkastus- oikeus vahvistettu	Pvm ja allekirjoitus
-------------------------------------	----------------------

Em. henkilöä koskevat tiedot	<input type="checkbox"/> Em. henkilölle on annettu tilaisuus tutustua häntä koskeviin tietoihin pvm: <input type="checkbox"/> Em. henkilölle on annettu häntä koskevat liitteenä olevat tiedot <input type="checkbox"/> henkilökohtaisesti, pvm: <input type="checkbox"/> lähetetty postitse, pvm: <input type="checkbox"/> Em. tietojen tarkastusoikeus evätty. Erillinen henkilötietolain 28 §:n mukainen kieltäytymistodistus perusteluineen annettu, pvm: <input type="checkbox"/> Em. henkilöstä ei ole tietoja rekisterissä.
Tietojen luovuttaja	Pvm ja allekirjoitus

Tarkastusoikeuden epäämisenä pidetään sitä, että rekisterinpitäjä ei ole kolmen kuukauden kuluessa antanut kirjallista vastausta rekisteröidylle (HetiL 28 §).

## Tietoturva asiakastietojen käsittelyssä

### Määritelmä ja sisältö

**Tietoturvalla** tarkoitetaan sellaisia hallinnollisia ja teknisiä toimenpiteitä, joiden avulla varmistetaan tietojen asianmukainen käsittely ja tietosuojan toteutuminen. Toimenpiteet kohdistuvat ennen kaikkea tietojen, tietojärjestelmien ja palveluiden luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen.

Asiakasasiakirjoja käytetään ainoastaan työtehtävissä ja salassa pidettäviä sekä arkaluontoisia tietoja koskeva vaitiolovelvollisuus sitoo työntekijää työ- tai palvelussuhteen päättymisen jälkeenkin. Ulkopuolisilla henkilöillä ei ole oikeutta asiakasasiakirjojen sisältämiin tietoihin.

### Tietojärjestelmien käytössä ja tietojen käsittelyssä huomioidaan mm.

- Salasanojen ja käyttäjätunnuksien huolellinen käsittely
- Näytön harkittu suuntaaminen työpisteessä
- Työtilan lukitseminen poissa ollessa
- Paperilla olevien asiakastietojen säilyttäminen lukitussa tilassa
- Salassa pidettävän materiaalin kopioimisen välttäminen
- Salassa pidettäviä tai luottamuksellisia tietoja ei saa lähettää sisäverkon ulkopuolelle sähköpostin välityksellä
- Asiakastietoihin tehtävien merkintöjen virheettömyydestä ja eheydestä huolehtiminen

## **Organisaation henkilöstö, käyttöoikeudet sekä tilat ja laitteet vaatimukset**

### **Henkilöstöä koskevat vaatimukset**

1. Henkilötietojen ja muiden VTJ-tietojen sekä tietoturvapoikkeamien käsittely ohjeistetaan ja koulutetaan organisaatiossa
2. Organisaatiossa on nimetty tietoturvallisuuden vastuhenkilö.
3. Henkilöstö toimii virkavastuulla tai muutoin sitoutuu kirjallisesti henkilö- ja VTJ-tietojen salassapitoon ja asianmukaiseen käsittelyyn.

### **Käyttöoikeuksia koskevat vaatimukset**

4. Käyttöoikeudet ovat henkilökohtaisia ja käyttöoikeuden haltija voidaan selvittää. Käyttöoikeuksien hallintaprosessit on kuvattu ja voimassaolon edellytykset tarkastetaan säännöllisesti.
5. Kirjautuminen järjestelmiin, joissa käsitellään tai voidaan nähdä palvelun välittämiä tietoja, tapahtuu tietoturvallisesti. Kirjautuminen tapahtuu salasanalla tai muutoin tietoturvallisesti tunnistautumalla. Salasanoja ja muita tunnistusvälineitä käsitellään tietoturvallisesti.

### **Tiloja ja laitteita koskevat vaatimukset**

6. Tilat ja laitteet, joissa käsitellään palvelun välittämiä tietoja, ovat sellaiset, että ulkopuoliset pääsevät tiloihin vain saatettuna ja heillä ei ole pääsyä palvelun välittämiin tietoihin.
7. Lisäksi varmistetaan, että poistettavilla ja huoltoon menevillä tietovälineillä ei ole palvelun välittämiä tietoja tai muita henkilötietoja.
8. Tilat ja laitteet ovat lukitut tai valvotut henkilöstön poissa ollessa taikka organisaatiossa on muu menettely, jolla varmistetaan, että ulkopuolisten näkymä henkilötietoihin on estetty.
9. Käytössä on palomuri ja ohjelmistopohjainen haittaohjelmasuojaus, jota päivitetään automaattisesti, tai muu menettelytapa, jolla varmistutaan haittaohjelmien ja vahingollisen liikenteen estämisestä.
10. Tietoliikenne, joka sisältää VTJ-tietoa ja henkilötietoja on salattu.
11. Tuotanto- ja testiympäristöt on eriytetty toisistaan.



Yllä kuvatut vaatimukset täyttyvät organisaatiomme.

## Henkilöstön salassapito ja -tietoturvasitoumus

### Kanervakodin salassapito- ja tietoturvasitoumus

---

#### Salassapito

- Sitoudun palvelusuhteeni tai muun työtehtäväni aikana sekä sen päätyttyä olemaan ilmaisematta sivulliselle tehtäviini liittyviä Kanervakodin asiakkaita, työntekijöitä, sopimuskumppaneita, muita yhteistyötahoja tai yksityisiä kansalaisia koskevia salassa pidettäviä tietoja, olivatpa ne minkä luonteisia hyvänsä, ellei asiakirjojen julkisuussäännöksistä tai asianomaisen antamasta suostumuksesta muuta johdu.
- Sitoudun noudattamaan erityistä huolellisuutta edellä tarkoitettujen salassa pidettävien tietojen ja niitä sisältävien tietomateriaalien kaikessa käytössä ja käsittelyssä.
- Sitoudun noudattamaan tietosuojaa ja salassapitoa koskevia lakeja, asetuksia, säännöksiä ja esimiesten antamia tietosuojamääräyksiä tietoturvallisuusperiaatteita ja -ohjeita.
- Asukkaiden henkilötietoja ei saa luovuttaa ulkopuolisille (esim. sähköpostin lähetys useammalle henkilölle, niin ettei muut näe vastaanottajia). Henkilötietoja saa lähettää vain salattuna sähköpostina.
- Tulkintatilanteissa kysyn neuvoa esimieheltäni tai muilta asiantuntijoilta.

#### Tietoturva

- Sitoudun seuraamaan ja noudattamaan kaikkia kulloinkin voimassa olevia tietoturvaohjeita.

#### Käyttäjätunnus ja salasana (koskevat tunnusten haltijoita)

- Kanervakodin työasemaa saa käyttää vain annetulla käyttäjätunnuksella ja salasanalla. Yhteistunnusten käytössä on noudatettava erityistä huolellisuutta ja noudatettava niiden käytöstä annettuja ohjeita.
- Käyttäjätunnus ja salasana on pidettävä muistissa, eikä niitä saa antaa muiden käyttöön. Uuden tunnuksen salasana on vaihdettava välittömästi ensimmäisen käyttökerran yhteydessä.
- Tietojärjestelmistä on kirjauduttava ulos tai työasema on lukittava välittömästi käytön jälkeen.
- Tietojärjestelmien käytöstä kertyy tietoa, josta ylläpitohenkilöstö voi tulla tietoiseksi. Järjestelmien käyttöä seurataan niiden omistajaorganisaatioissa.

#### Työaseman käyttö (koskee käyttöön oikeutettuja)

- Työasemassa saa vain käyttää Kanervakodin vakioympäristöön käytettäväksi määriteltäviä, lisensoituja ohjelmistoja.
- Ohjelmia ei saa kopioida eikä käyttää työpaikan ulkopuolella.
- Levykkeiden ja muiden tietovälineiden käytön yhteydessä on varmistettava niiden viruksettomuudesta.



KANERVAKOTI - Kanervahemmet ry  
ANKKURISAARENTIE 4-6  
02160 ESPOO

Y-tunnus: 0221424-9

Puh: 050 5692873

toiminnanjohtaja@kanervakoti.fi

- Tietokoneviruksen saastuma työasema on suljettava välittömästi ja asiasta ilmoitettava IT tukeen.
- Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Palvelimet varmistetaan keskitetysti.

### **Toimenpiteet työsuhteen tai toimeksiannon päättyessä**

- Työsuhteen tai muun työtehtävän päätyttyä palautan kaiken käyttööni saamani Kanervakodin tai kolmannen osapuolen omaisuuden esimerkiksi asiakirjat, kirjalliset materiaalit, käsikirjat, ohjelmistot ja niistä tehdyt jäljennökset, laitteet, kulunvalvontakortit, avaimet, luottokortit ja muut mahdolliset välineet. Kanervakodin verkkolevyllä tai muualla olevan materiaalin kopiointi palvelussuhteensa päättävälle henkilölle myöhempää käyttöä varten on kielletty.

### **Seuraamukset**

- Vaitiolo- ja tietoturvasitoumuksen rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle ja toiminnanjohtajalle.
- Sitoumuksen rikkomisesta voi olla seurauksena huomautus, kirjallinen varoitus, palvelussuhteen päättäminen, vahingonkorvausvelvollisuus, rikosoikeudellinen seuraamus tai muu lainmukainen seuraamus.

**Olen lukenut tämän salassapito- ja tietoturvasitoumuksen ja allekirjoituksellani sitoudun sitä noudattamaan.**

Työntekijän allekirjoitus \_\_\_\_\_

Nimenselvennys \_\_\_\_\_

Henkilötunnus \_\_\_\_\_

Paikkakunta, pvm \_\_\_\_\_

### **Tietoturvan omavalvontasuunnitelman allekirjoitus**

Toiminnanjohtajan allekirjoitus \_\_\_\_\_

Nimenselvennys Tarja Kiesi

Paikkakunta, pvm \_\_\_\_\_