

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

HENKILÖTIETOJEN KÄSITTELYOHJE

1. Ohjeen tarkoitus

Henkilötietojen käsittelyohje perustuu EU:n yleiseen tietosuoja-asetukseen (EU 679/2016) ja Tietosuojalakiin (1050/2018). Henkilötietojen käsittelyohjeen tarkoituksena on ohjeistaa palveluntuottajia, jotka käsittelevät henkilötietoja hyvinvointialueen lukuun. Keski-Uudenmaan hyvinvointialue toimii sopimuksen nojalla rekisterinpitäjänä ja palveluntuottaja toimii henkilötietojen käsitteijänä.

Keskeiset käsitteet

Käsitteet on määritelty EU:n yleisessä tietosuoja-asetuksessa

<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679>

<https://www.privacy-regulation.eu/fi/4.htm>

PDF-muodossa: <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=FI>

2. Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyssä sopijapuolten on noudatettava voimassa olevan kansallisen ja EU-tietosuojalainsäädännön vaatimuksia, mukaan lukien EU:n yleisen tietosuoja-asetuksen vaatimukset ja osapuolten välille laadittu tietosuojasopimus.

Tällä ohjeella rekisterinpitäjä tarkentaa käsittelyn periaatteita ja menettelytapoja.

Rekisterinpitäjä vastaa ja sen on pystyttävä osoittamaan, että tietosuoja-asetuksen 5 artiklan 1 kohdan mukaisia käsittelyn periaatteita noudatetaan palvelun tuottamisessa. Rekisterinpitäjää velvoittavat käsittelyn periaatteet on kuvattu alla lihavoidulla tekstillä ja tarkennettu sisennetyin nuolimerkinnoin.

1. Tietoja on käsiteltävä rekisterinpitäjän ohjeistuksen mukaisesti ja rekisteröidyn kannalta läpinäkyvästi

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

- Käsittelijä sitoutuu noudattamaan osapuolten välille laadittua tietosuojasopimusta.
- Käsittelijä käsittelee tietoja rekisterinpitäjän ohjeistuksen mukaisesti.
- Rekisterinpitäjä ja käsittelijä sopivat henkilötietojen käsittelystä henkilötietojen käsittelytoimien kuvauksella (Tietosuojasopimuksen liite 1.2).

2. Tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla

- Henkilötietojen käyttö on sallittu vain henkilötietojen käsittelyn kuvauksessa määriteltyyn tarkoitukseen.

3. Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään

- Rekisterinpitäjä määrittelee käsiteltävät tiedot.

4. Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä

- Käsittelijä suorittaa edellä mainitut toimenpiteet vain rekisterinpitäjän pyynnöstä.

5. Tiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten

- Käsittelystä ja sen kestosta on sovittu Henkilötietojen käsittelyn kuvauksessa.
- Säilytysajat määrittelee rekisterinpitäjä.

6. Tietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia

- Käsittelijän tulee toteuttaa sovitut tekniset ja organisatoriset turvatoimet ja osoittaa niiden toteuttaminen siten kuin tietoturvaliitteessä (Pääsopimuksen liite 2) on tarkemmin sovittu tai sopijapuolten erikseen sopimalla tavalla.

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

- ➔ **Henkilötietojen käsittelijän tulee huomioida kaikessa käsittelyn vaiheessa, että henkilötiedot ovat suojattu samalla suojaustasolla kuin ne ovat järjestelmässä esim. siirrettävät asiakas-/potilastiedot ovat koko prosessin aikana salattuna.**

3. Tietojen suojaaminen

Henkilötietojen käsittelijän on toteutettava sovitun mukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelemiseltä. Sopijapuolet tarkistavat ja päivittävät näitä toimenpiteitä tarvittaessa. Rekisterinpitäjä kommunikoi käsittelijälle riskitason ja riskitasoa vastaavat toimenpiteet.

Tietojen suojaamiseksi on huolehdittava mm. siitä, että:

- 1. Henkilötietojen tekninen suojaaminen on hoidettu**
- 2. Henkilötietojen käsittelijän palomuurit, virustorjunta, salausjärjestelmät, langattomat yhteydet ym. tekninen tietoturva on yhdessä sovitun alan yleisen tietoturvakäytännön mukaisessa kunnossa.**
- 3. Henkilötietojen käsittelijällä on menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.**
- 4. Käsittelijän toimista jää asianmukaiset lokimerkinnät, jotka tulee olla rekisterinpitäjän saatavilla.**
- 5. Henkilötietojen käsittelijä pystyy takaamaan käsittelyjärjestelmien ja palveluiden jatkuvan luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden.**
- 6. Mikäli palveluntuottaja käyttää palvelun tuottamisessa alihankkijoita, toimittaja vastaa alihankkijoiden toiminnasta kuten omastaan. Muutokset alihankkijoihin tulee hyväksyttävä rekisterinpitäjällä.**
- 7. Henkilötietojen käsittelijä pystyy palauttamaan nopeasti tietojen saatavuuden sekä pääsyn tietoihin fyysisen tai teknisen vian sattuessa.**

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

8. Henkilötietojen käsittelijä on määritellyt työtehtävät ja henkilöt, jotka käsittelevät työtehtäviensä vuoksi rekisterinpitäjän henkilötietoja. Henkilökuntaa on koulutettu ja käytössä on vaitiolositoumus, velvoite jatkuu myös käsittelijän/työntekijän poistuessa työnantajan/palveluntuottajan palveluksesta

- ➔ Käsittelijän tulee osoittaa tarvittaessa dokumentaatiolla, kenellä henkilötietojen käsittelijän henkilöillä on oikeus rekisterinpitäjän henkilötietojen käsittelyyn ja millä tasolla.
- ➔ Rekisterinpitäjä määrittelee henkilöt, joilla on oikeus tehdä palvelupyynnöitä käsittelijälle.
- ➔ Vain rekisterinpitäjä voi antaa palvelupyynnön ja luvan henkilötietojen käsittelyyn.

4. Henkilötietojen tietoturvaloukkausta koskeva ilmoitusvelvollisuus

Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

- ➔ Henkilötietojen käsittelijän ilmoitusvelvollisuus on kuvattu Tietosuojasopimuksessa. Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle kirjallisesti ja lisäksi millä tahansa muulla sopivalla tavalla (esim. puhelimitse) ilman aiheetonta viivytystä sen tietoon tulleesta tietoturvaloukkauksesta.
- ➔ Ilmoitus tulee tehdä puhelimitse tai sähköpostilla alla oleviin osoitteisiin:

Tietosuojavastaava Satu Jokinen, 050 497 2639, tietosuojavastaava@keusote.fi

Tietoturvapääällikkö Timo Pirttilä, 050 497 2496, timo.pirttila@keusote.fi

Tietohallintojohtaja Antti Ylä-Jarkko, 050 497 2514, antti.yla-jarkko@keusote.fi

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

5. Erityisiä henkilötietoryhmiä koskeva käsittely

Tietosuojasetuksen 9 artiklan mukaan sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittinen suuntautuminen, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä.

Henkilötietojen käsittelijän tulee käsitellä erityisiä henkilötietoryhmiä erityistä huolellisuutta noudattaen.

- ➔ Henkilötietojen käsittelijä käsittelee salassa pidettävää ja erityisiä henkilötietoja koskevia tietoja rekisterinpitäjän antaman ohjeistuksen mukaan.

6. Salassa pidettävien tietojen käsittely ja säilyttäminen

Jokaisen rekisterinpitäjän työntekijän tai rekisterinpitäjän lukuun toimivan on huolehdittava, että salassa pidettävien tietojen ja asiakirjojen käsittely ja säilytys toteutetaan tämän ohjeen mukaisesti.

Asiakirjojen salassapito perustuu joko Lakiin viranomaisen toiminnan julkisuudesta 621/1999 (julkisuuslaki) tai muuhun lakiin asiakirjan salassapidosta. Asiakirjat tai tietosisällöt voivat muodostua salassa pidettäväksi, kun niitä yhdistetään esim. tietokannoiksi.

Karkeasti määritellen salassa pidettäviä tietoja ovat kaikki potilastiedot ja muut arkaluonteiset tiedot, yrityssalaisuudet ja julkisuuslain mukaan salassa pidettävät tiedot, kuten henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista.

Salassa pidettävät asiakirjat eivät ole julkisia vaan salassapitoperusteen mukaisesti salassa pidettäviä. Asiakirjasta saa antaa tietoja vain niille henkilöille, joille on myönnetty oikeus käsitellä asiakirjan edellyttämän suojaustason mukaisia asiakirjoja ja joilla on asiakirjan sisältämää tietoa edellyttävä, työtehtäviin pohjautuva käsittelytarve. Henkilön tulee tuntea salassa pidettävien tietoaineistojen käsittelysäännöt. Henkilötietojen

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

käsittelijä vastaa siitä, että ympäristö, jossa tietoja käsitellään, tulee olla turvallisuusjärjestelyin suojattu.

Käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

- ➔ Julkisuuslaissa on 32-kohtainen luettelo yleisimmistä salassapitoperusteista (24 §). Esimerkiksi kaikki sosiaali- ja terveydenhuollon ja työhallinnon asiakastiedot, oppilaan ja hänen perheensä henkilökohtaisia oloja sekä oppilashuoltoa koskevat tiedot ovat aina salassa pidettäviä. Myös tiedot yksityiselämän piirissä esitetyistä mielipiteistä, elintavoista, yhdistys - tai harrastustoiminnasta, perhe-elämästä sekä niihin verrattavista henkilökohtaisista oloista ovat salassa pidettäviä. Esimerkiksi jokaisen perhesuhteet sekä yksityishenkilön tai työntekijän puoluekanta tai jäsenyys ammatti- tai muuhun yhdistykseen ovat salassa pidettävä tietoja.
- ➔ Salassa pidettäviä tietoja ei saa panna yleisesti nähtäväksi. Niitä ei saa laittaa myöskään internetiin eikä julkaista tai antaa sivullisille luvatta muullakaan tavoin. Salassa pidettäviä tietoja sisältäviä asiakirjoja ei saa luvatta laittaa myöskään sisäiseen verkkoon.
- ➔ Arkistotoimen sisällöstä ja järjestämisestä säädetään arkistolaissa. Arkistolaitos määrää, mitkä asiakirjat tai niiden sisältämät tiedot säilytään pysyvästi. Muutoin rekisterinpitäjä määrää asiakirjojen säilytysajat ja -tavat sekä ylläpitää niistä arkistonmuodostussuunnitelmaa.
- ➔ Määräajan säilytettävät asiakirjat tulee hävittää niille määrätyn säilytysajan jälkeen siten, että tietosuoja on varmistettu.
- ➔ Rekisterinpitäjä huolehtii tarpeettomiksi käyneiden henkilötietojen poistamisesta henkilörekistereistä. Myös tarpeettomaksi käynyt henkilörekisteri on hävitettävä, jollei sitä ole määräysten mukaan edelleen säilytettävä eikä sitä siirretä arkistoon. Henkilörekistereiden hävittämisestä, siirtämisestä arkistoon sekä muun muassa arkistoon siirrettyjen henkilörekistereiden käytöstä ja tietojen luovuttamisesta noudatetaan tietosuojalainsäädäntöä.

7. Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä rekisteröidyn antamalla suostumuksella tai, jos käsittelystä säädetään laissa (Tietosuojalaki 1050/2018, § 29).

HENKILÖTIETOJEN KÄSITTELYOHJE

Tietosuojasopimuksen liite 1.1

1.1.2023

- ➔ Rekisterinpitäjä määrittelee, mihin henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin on tarpeellista tulostaa henkilötunnus. Henkilötietojen käsittelijä noudattaa rekisterinpitäjän ohjeistusta.

8. Henkilötietojen asianmukainen hävittäminen

Tiedot tulee hävittää tietosuoja ja tietoturva varmistuen niin, että tiedot eivät joudu asiattomien käsiin. Lisäksi manuaaliset ja sähköiset asiakirjat tulee hävittää tietoturvallisesti siten, että niitä ei enää voida yhdistää luonnolliseen henkilöön. Virheelliset ja vanhentuneet tiedot tulee hävittää välittömästi.

- ➔ Rekisterinpitäjä indikoi, mitkä tiedot ovat virheellisiä ja vanhentuneita.
- ➔ Palvelupyynnön perusteella henkilötietojen käsittelijä tekee toimenpiteet, huomioiden myös sovittu mukaisen säilytysajan.
- ➔ Pyynnöt tietojen korjaukseen tai poistamiseen tulevat aina rekisterinpitäjältä.
- ➔ Henkilötietojen hävittämisestä on sovittu Henkilötietojen käsittelyä koskevassa kuvauksessa.

9. Salassapito ja vaitiolovelvollisuus

Henkilötietojen käsittelijä on velvollinen pitämään salassa sopimussuhteen aikana tietoonsa saamat henkilötiedot ja vaitiolovelvollisuus jatkuu sopimussuhteen päätyttyä.

- ➔ Salassapidosta on sovittu osana Sopimusta.
- ➔ Henkilötietojen salassapitoaika on määritelty lainsäädännössä.
- ➔ Sopijapuoli vastaa siitä, että sen työntekijät ovat sitoutuneet salassapitovelvollisuuteen.