

## TIETOSUOJASELOSTE

Yleinen tietosuoja-asetus (2016/679)

Laatimispäivä 24.04.2018

## Rekisterinpitäjä

Palvelunjärjestäjien omistama Kuntien Tiera Oy on asiakasrekisterin tekninen hallinnoija ja tämän rekisteriselosteen ylläpitäjä. Kukin järjestelmää käyttävä palvelunjärjestäjä on rekisterinpitäjä omien asiakkaiden asiakastiedoille, joita järjestelmässä käsitellään. Digia Finland Oy on asiakastietoja käsittelevän järjestelmän ylläpitäjä.

Nimi: Kuntien Tiera Oy

Y-tunnus: 2362180-3

Osoite: Tammasaarenkatu 3

Postinumero: 00180

Postitoimipaikka: Helsinki

Puhelinnumero: 020 734 7777

## Rekisteriasioita hoitava henkilö

Yritys: Kuntien Tiera Oy

Nimi: Jani Grönberg

Osoite: Tykistökatu 4 A

Postinumero: 20520

Postitoimipaikka: Turku

Sähköpostiosoite: jani.gronberg@tiera.fi

## Rekisterin nimi

Palveluseteli- ja ostopalvelujärjestelmän asiakasrekisteri

## Rekisterinpitäjät, joiden lukuun henkilötietoja käsitellään

PSOP-järjestelmää käyttämien palvelunjärjestäjien yhteystiedot löytyvät [parastapalvelua.fi-sivuilta](http://parastapalvelua.fi-sivuilta).

0

## Rekisterin käyttötarkoitus

Palveluseteli- ja ostopalvelujärjestelmä (PSOP) on palvelunjärjestäjien käytävissä oleva tietojärjestelmä, jonka avulla hallinnoidaan eri palvelunjärjestäjien ja eri palvelualueiden ostopalvelu- ja palveluseteliasiakkaiden palveluiden järjestämiseen liittyviä tietoja.

Henkilötietojen käsittelyn tarkoituksena PSOP-järjestelmässä on asiakkaan yksilöiminen. Henkilötietojen kerääminen perustuu sopimukseen ostovoiman myöntäjän eli palvelunjärjestäjän ja asiakkaan eli kuntalaisen välillä.

Tiedot koostuvat asiakastiedoista, ja eri ostovoimiin (mm. palveluseteli, ostopalvelu, asiakasseteli ja henkilökohtainen budjetti) liitetyistä palvelutiedoista, joissa näkyvät asiakkaalle myönnetyn palvelun sisältö ja määrä.

Asiakastiedot erotetaan järjestelmässä palvelunjärjestäjä- ja palvelukohtaisesti. Asiakastiedot kytkeytyvät aina johonkin palveluun, ja palvelu kertoo, minkä asiakasrekisterin tiedosta on kysymys.

Palveluntuottajat kirjaavat asiakkaille antamansa palvelut järjestelmään. Kirjausten perusteella järjestelmässä muodostuu tilitysaineisto palveluntuottajalle kuuluvan korvauksen suorittamista varten.

## Rekisterin sisältämät henkilötietoryhmät

Henkilötietoryhmät, joiden tietoja voidaan käsitellä, ovat ostovoiman järjestelmän kautta saava asiakas, asiakkaan puolesta-asioijana toimivat henkilöt, palveluntuottajana toimivan yrityksen työntekijät, sekä palvelunjärjestäjältä käyttäjätunnuksen saavat työntekijät ja tahot.

Asiakkaasta kerätään seuraavaa tietoa:

- etunimet, sukunimi
- henkilötunnus
- osoitetiedot: katuosoite, postilokero-osoite, kadunnimi, huoneistotunnuksen numero, huoneistotunnuksen kirjainosa, huoneistotunnuksen jakokirjain, postinumero, postitoimipaikka, osoitetaranne, kunta, maakoodi

- sukupuoli
- kotikuntanumero
- kuntaan muuttamispäivä, poismuuttamispäivä
- kuolinpäivä
- asiointikieli
- lähiomaisen nimi ja puhelinnumero
- asiakkaalle myönnetty palvelut ja niiden määrät sekä mahdolliset lisätiedot, joita palveluntuottaja tarvitsee palvelua antaakseen

Puolesta-asiointioikeuden saaneista henkilöistä kerätään seuraavaa tietoa:

- etunimi
- sukunimi
- henkilötunnus
- puhelinnumero
- sähköpostiosoite

Palveluntuottajien työntekijöistä kerätään seuraavaa tietoa:

- palveluntuottajien Katso-nimenkirjoitusoikeudelliset henkilöt
  - nimi
  - sähköpostiosoite
  - Katso-nimenkirjoitusoikeus
  - palvelukohtainen käyttövaltuus
- palveluntuottajien järjestelmään kirjautuvat käyttäjät:
  - nimi
  - sähköpostiosoite
  - käyttäjärooli
  - palvelukohtainen käyttövaltuus
- palveluntuottajan järjestelmään tallennettujen palvelua tuottavat työntekijät:
  - nimi
  - henkilötunnus
  - ammattinimike
  - toimenkuva
  - rekisteröintinumero
  - puhelinnumero ja sähköposti, jos kyseinen henkilö toimii myös yhteyshenkilönä
- palveluntuottajien yrityksen tai yrityksen osan yhteyshenkilöt
  - nimi
  - puhelinnumero
  - sähköpostiosoite

Palvelunjärjestäjän työntekijöistä ja palvelunjärjestäjän myöntämien käyttäjätunnuksien saaneista henkilöistä kerätään seuraavaa tietoa:

- nimi
- sähköpostiosoite
- käyttäjärooli
- palvelukohtainen käyttövaltuus

## Tietojen säilytysaika

PSOP-järjestelmässä säilytettävien tietojen käsittely ja vähimmäisaika määräytyvät mm. seuraavien lakien mukaan:

- Suomen perustuslaki (731/1999)
- Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki)
- Laki yksityisyyden suojasta työelämässä (759/2004, ns. työelämän tietosuojalaki)
- Laki potilaan asemasta ja oikeuksista (785/1992, potilaslaki)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, asiakaslaki)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Henkilötietolaki (523/1999) 24.5.2018 asti
- Yleinen tietosuojasetus (2016/679) 25.5.2018 alkaen

Asiakstieto syntyy ensimmäisen kerran asiakkaalle palveluseteliä, ostopalvelua, asiakasseteliä, henkilökohtaista budjettia, tai muuta ostovoimaa myönnettäessä. Asiakkaan henkilötiedot haetaan Väestötietokeskuksen ylläpitämästä väestötietojärjestelmästä rajapinnan kautta. Asiakas voi itse ylläpitää sähköpostiosoitetta, puhelinnumeroa, ja tietoa lähiomaisesta.

Asiakstietoja säilytetään PSOP-järjestelmässä lain määräämän ajan mukaisesti. Lain määräämä säilytysaika on korkeintaan 12 vuotta viimeisestä palvelutapahtumasta tai asiakkaan kuolemasta. Säilytysajan päättymisen jälkeen tiedot poistetaan.

## Säännönmukaiset tietolähteet

Asiakstieto tallennetaan PSOPiin siinä vaiheessa, kun hänelle on palvelunjärjestäjän toimesta myönnetty palveluseteli tai ostopalvelu. Uusien asiakkaiden osalta, palvelunjärjestäjän viranomaisen lisäksi asiakkaan tietoihin henkilötunnuksen, tai henkilötunnus saadaan perusjärjestelmästä palvelunjärjestäjällä tehdyn päätöksen perusteella. Henkilötunnuksen perusteella suoritetaan haku Väestötietojärjestelmään (VRK/VTJ), josta saadaan asiakkaan ajantasaiset väestötiedot. Turvakielto-statuksella olevien henkilöiden osoitetietoja ei tuoda/tallenneta PSOPiin. Asiakstietoa ylläpidetään viikoittaisella päivityksellä Väestötietojärjestelmästä.

### PSOPin tietolähteet

Asiakas: Asiakkaalla on mahdollisuus täyttää järjestelmään oma sähköpostiosoitteensa ja puhelinnumeron, sekä lähiomaisen nimen ja puhelinnumeron.

Palvelunjärjestäjä: Asiakkaan henkilötunnus, sekä asiakkaalle myönnetty palvelu, siirretään palvelunjärjestäjien perusjärjestelmästä PSOP-järjestelmään joko palvelunjärjestäjän työntekijöiden tai järjestelmäintegraation kautta.

Väestötietojärjestelmä: Asiakastiedot (asiakkaan osoitetiedot), palveluseteli- ja/tai ostopalvelujen piirissä olevien asiakkaiden muutostiedot: kuolleet, kuntaa vaihtaneet asiakkaat. Turvakielollisen asiakkaan osoitetietoja ei palauteta VTJ:stä kyselyssä.

Kanta-palvelut: Ostopalvelun valtuutus. Valtuutuksen myötä terveydenhuollon palveluja asiakkaalle tuottava yksityinen palveluntuottaja saa nähdäkseen asiaa ja asiakasta koskevat kunnan tekemät hoitotiedot. Valtuutuksen avulla kunta saa käyttöönsä uudet, yksityisen palveluntuottajan tekemät ko. asiakasta ko. asiassa koskevat kirjaukset.

Suomen Tilaajavastuun palvelu: PSOP-järjestelmä saa Tilaajavastuun palvelun kautta tiedon yksityisiä palveluntuottajia koskevista lakisääteisen valvonnan edellyttämistä tiedoista. Sähköinen ja automaattinen valvonta kohdistuu suostumuksen antaneisiin yrityksiin. Muut tuottajat ovat manuaalisen valvonnan piirissä.

KATSO-tunnistus: Katso-tunnistuspalvelusta tuodaan palveluntuottajan Y-tunnus, sekä Y-tunnuksen hallinnointioikeus palveluntuottajan kirjautuessa järjestelmään kyseisillä tunnuksilla.

Suomi.fi -tunnistuspalvelut: Suomi.fi -tunnistuspalveluista tuodaan asiakkaan henkilötunnus asiakkaan kirjautuessa pankkitunnuksilla tai mobiilivarmenteella.

Suomi.fi -valtuudet: Suomi.fi-valtuudet -palvelusta tuodaan alle 10-vuotiaan puolesta-asioitavan lapsen henkilötunnus huoltajan kirjautuessa järjestelmään omalla henkilötunnuksellaan.

## Tietojen säännönmukaiset luovutukset

Eri rekistereiden tietoja ei yhdistellä PSOPissa, eikä niitä luovuteta eteenpäin.

## Tietojen siirto EU:n tai ETA:n ulkopuolelle

PSOP-järjestelmän asiakasrekisterin tietoja ei siirretä EU:n tai ETA:n ulkopuolelle

## Rekisterin suojausten periaatteet

PSOP- järjestelmä on selainkäyttöinen. Käyttöoikeudet on määritelty palvelunjärjestäjä- ja palvelukohtaisesti. Palvelunjärjestäjän työntekijät pääsevät käsittelemään vain sen palvelunjärjestäjän rekisterin tietoja, jonka palveluita he järjestävät. Käyttäjätunnuksukset ovat henkilökohtaisia, ja käyttöoikeus poistetaan, kun henkilö siirtyy toisiin tehtäviin tai työsuhde päättyy.

Yksityisen palveluntuottajan oikeus käyttää asiakastietoja perustuu siihen, että palveluntuottaja toimii palveluita järjestävän palvelunjärjestäjän lukuun palveluntuottajana. Palveluntuottaja pääsee näkemään vain sen asiakkaan tietoja, johon on asiakassuhde. Käyttäjätunnuksukset ovat henkilökohtaisia.

Asiakas itse tai valtuutettu puolesta-asioija voi nähdä vain omat tietonsa. Kirjautuminen järjestelmään vaatii vahvan tunnistautumisen.

Tietojärjestelmä sekä tiedostot on suojattu teknisillä suojausmenetelmillä. Asiakastietoja sisältävän järjestelmäosan käyttöön ja asiakastietojen muuttamiseen ovat oikeutettuja vain ne työntekijät, joilla työnsä puolesta on oikeus käsitellä asiakastietoja. Heitä sitoo vaitiolovelvollisuus. Kullakin käyttäjällä on oma käyttäjätunnus ja salasana järjestelmään. Henkilökohtaisen käyttäjätunnuksen ja salasanan perusteella pystytään todentamaan kaikki sisään kirjautumiset ja käyttäjän tekemät tapahtumat.

Käyttäjille on määritelty käyttöoikeustaso, joten tietoja pääsee muokkaamaan vain nimetyt käyttäjät.

Työtiloissa liikkumista valvotaan kulkuluvilla (koskee toimittajan työtiloja, jossa järjestelmän laitekanta sijaitsee).

Tiedot kerätään tietokantoihin, jotka ovat palomuurein, salasanoin ja muin teknisin keinoin suojattuja. Tietokantaan tallennetut henkilötiedot ovat kryptattuna.

Tietokannat ja sovelluspalvelimet sijaitsevat lukituissa ja vartioiduissa tiloissa ja tietoihin pääsevät käsiksi vain tietyt ennalta nimetyt henkilöt henkilökohtaisilla tunnuksillaan.

Järjestelmän käytöstä syntyy lokirekisteri, joka on järjestelmän ylläpitäjän hallinnassa. Kaikesta henkilön tietojen käsittelystä tehdään aina erilliset merkinnät.

### Evästeiden käyttö PSOP-järjestelmässä:

PSOP-järjestelmä käyttää evästeitä vain yhden istunnon ajan, ja evästeissä ei kuljeteta muuta tietoa kuin käyttäjäistunnon tunnisteen tieto. Järjestelmäpäivityksen myötä PSOP-järjestelmässä tulee käyttöön eväste, jonka elinaika on yhden istunnon ajan, ja joka sisältää seuraavat tiedot:

- Käyttäjän nimi
- Käyttäjän sisäinen tietokantaid
- Käyttäjän sisäinen tietokantatunniste
- Organisaation nimi johon käyttäjä kuuluu (Palvelunjärjestäjä / palveluntuottaja)
- Organisaation PSOP kotisivun osoite
- Organisaation tietokantaid
- Roolit joita käyttäjällä PSOPissa on
- Tietojen hyväksyty elinaika
- Tietojen sähköinen allekirjoitus

---

3

Uudessa evästeessä ei tulla säilyttämään salaista tietoa, eikä evästeitä käytetä järjestelmässä käyttäjien profilointiin, vaan tiedot liittyvät käyttäjäistunnon hallintaan.

## Rekisteröidyn oikeudet

### Rekisteröidyn oikeus hänestä kerättyihin tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy PSOP-järjestelmän asiakasrekisteriin tallennettuihin henkilötietoihin.

Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.

Tarkastusoikeus voidaan evätä vain laissa mainituilla perusteilla. Epäämisperusteena voi olla esimerkiksi, että tiedon antamisesta saattaisi aiheutua vaaraa rekisteröidylle tai jonkun muun oikeuksille. Jos tarkastusoikeus evätään, asiakkaalle annetaan kirjallinen kieltäytymistodistus, josta ilmenee kieltäytymisen peruste. Ratkaisuun tyytymätön voi viedä asian tietosuojaa valvovan viranomaisen ratkaistavaksi.

Rekisteritietojen tarkastuspyyntö tehdään omakätisesti allekirjoitetulla tai vastaavalla tavalla varmennetulla asiakirjalla taikka henkilökohtaisesti rekisterinpitäjän luona. Tarkastuspyyntö toimitetaan oman palvelunjärjestäjän tietosuojavastaavalle, tai rekisteriasioista vastaavalle yhteyshenkilölle tai taholle. PSOP-järjestelmää käyttävien palvelunjärjestäjien sivustoilta löytyvät palvelunjärjestäjäkohtaiset asiakastietojen rekisteriselosteet ja palvelunjärjestäjien yhteyshenkilöt.

### Oikeus vaatia tiedon korjaamista

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheutonta viivytystä rekisteröityä koskevat PSOP-järjestelmän asiakasrekisteriin tallennetut epätarkat ja virheelliset henkilötiedot.

Korjauspyyntö tehdään omakätisesti allekirjoitetulla tai vastaavalla tavalla varmennetulla asiakirjalla taikka henkilökohtaisesti rekisterinpitäjän luona. Pyynnössä on syytä tarkasti yksilöidä ja perustella, mitä tietoa vaaditaan korjattavaksi, mikä on asiakkaan mielestä oikea tieto ja millä tavoin korjaus pyydetään tekemään. Korjatusta tiedosta, korjauksen tekijästä sekä korjauspäivämäärästä jää rekisteriin tieto. Alkuperäinen merkintä on mahdollista nähdä jälkikäteen.

Jos tiedon korjaamisesta kieltäydytään, asiakkaalle annetaan kirjallinen kieltäytymistodistus, josta ilmenee kieltäytymisen peruste. Ratkaisuun tyytymätön voi viedä asian tietosuojaa valvovan viranomaisen ratkaistavaksi.

Rekisteritietojen korjauspyyntö toimitetaan oman palvelunjärjestäjän tietosuojavastaavalle, tai rekisteriasioista vastaavalle yhteyshenkilölle tai taholle. PSOP-järjestelmää käyttävien palvelunjärjestäjien sivustoilta löytyvät palvelunjärjestäjäkohtaiset asiakastietojen rekisteriselosteet ja palvelunjärjestäjien yhteyshenkilöt.

### Muut henkilötietojen käsittelyyn liittyvät oikeudet

PSOP-järjestelmässä henkilötietoja ei käsitellä profilointi- tai suoramarkkinointitarkoituksessa.