LIITE 3. HENKILÖTIETOJEN KÄSITTELYN EHDOT

1. Määritelmät

Tässä liitteessä käytetään seuraavia määritelmiä

**Henkilötieto**

tarkoittaa tietosuoja-asetuksen mukaisia henkilötietoja, joita ovat kaikki tunnistettavaan tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot.

**Henkilötietojen käsittelijä**

tarkoittaa tietosuoja-asetuksen mukaista henkilötietojen käsittelijää, joka on rekisterinpitäjästä ulkopuolinen, henkilötietoja rekisterinpitäjän lukuun käsittelevä taho. Tässä liitteessä henkilötietojen käsittelijästä käytetään nimitystä palveluntuottaja.

**Palveluntuottaja**

tarkoittaa palveluntuottajaa, joka on hyväksytty kunnan palvelunsetelituottajien rekisteriin.

**Rekisterinpitäjä**

tarkoittaa tietosuoja-asetuksen mukaista rekisterinpitäjää, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjänä toimii kunta.

**Rekisteröity**

tarkoittaa luonnollista henkilöä, jota henkilötieto koskee.

**Osapuoli**

 tarkoittaa kuntaa palvelusetelipalvelun järjestäjänä ja palveluntuottajaa sen tuottajana.

**Tietosuoja**

tarkoittaa tietosuoja-asetuksen ja tietosuojalain (1050/2018) mukaista sisäänrakennettua ja oletusarvoista tietosuojaa.

**Tietosuoja-asetus**

 tarkoittaa EU:n yleista tietosuoja-asetusta (EU)2016/679.

**Tietosuojasääntely**

tarkoittaa tietosuoja-asetuksen ja sitä täydentävän kansallisen tietosuojalain (1050/2018) mukaista sääntelyä sekä niiden perusteella annettuja toimivaltaisten viranomaisten ratkaisuja.

**Kunnan henkilötieto**

 tarkoittaa henkilötietoa, joista kunta vastaa rekisterinpitäjänä.

1. Sitoumuksen merkitys

Palveluntuottaja sitoutuu kunnan palvelusetelituottajana tekemänsä hakemuksen mukaisesti toteuttamaan henkilötietojen käsittelyn ja tietosuojaa koskevat tehtävät ja toimenpiteet tämän sitoumuksen mukaisesti.

Kunta ei maksa palveluntuottajalle henkilötietojen käsittelystä erillistä korvausta.

1. **Yhteyshenkilöt tietosuoja-asioissa**

Palveluntuottaja nimeää tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön kunnan henkilötietoihin liittyviä yhteydenottoja varten.

Kunta nimeää oman yhteyshenkilönsä tietosuojaan liittyviä asioita varten.

Kunnan yhteyshenkilö tietosuoja-asioissa:

Someron kaupungin tietosuojavastaava Sami Kaven

p. 044-7791292
tietosuojavastaava@somero.fi

Palveluntuottajan on ilmoitettava yhteyshenkilön muutoksista viipymättä kunnan yhteyshenkilölle.

1. Osapuolten roolit henkilötietojen käsittelyssä

Kunta toimii tietosuojasääntelyn mukaisena rekisterinpitäjänä.

Palveluntuottaja toimii henkilötietojen käsittelijänä, joka käsittelee henkilötietoja kunnan puolesta ja lukuun.

Kunta vastaa siitä, että se noudattaa omassa toiminnassaan tietosuojasääntelyä ja pyrkii kaikin kohtuullisin keinoin myötävaikuttamaan palveluntuottajan mahdollisuuksia toimia tämän liitteen mukaisesti.

1. Palveluntuottajan velvollisuudet
	1. Palveluntuottajan yleiset velvollisuudet

Palveluntuottaja noudattaa kulloinkin voimassa olevan tietosuojasääntelyn edellyttämiä menettelytapoja ja henkilötietojen käsittelyä ja suojaamista koskevia säännöksiä, sitoumuksen ehtoja ja kunnan ohjeita. Palveluntuottaja vastaa siitä, että palvelu on tietosuoja-asetuksen, sitä täydentävän tietosuojalainsäädännön ja sitoumuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta on säädetty.

Palveluntuottaja sitoutuu toteuttamaan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn turvallisuuden ja rekisteröityjen oikeuksien toteutumisen varmistamiseksi.

Palveluntuottajan on tällöin huomioitava käsittelyn ja käsiteltävien henkilötietojen luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröidyn oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Edellä mainittujen toimenpiteiden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä käsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa.

Mitä tässä sitoumuksessa sovitaan henkilötietojen käsittelystä, koskee myös pääsyn mahdollistamista kunnan henkilötietoihin esimerkiksi hallinta- ja valvontayhteyden välityksellä.

* 1. Henkilötietojen käsittelyn laajuus

Palveluntuottaja käsittelee kunnan henkilötietoja sitoumuksen kohteen mukaisessa tarkoituksessa ja laajuudessa. Palveluntuottaja ei käsittele eikä muulla tavoin hyödynnä sitoumuksen perusteella käsittelemiään henkilötietoja muutoin kuin sitoumuksen täyttämisen mukaisessa tarkoituksessa ja laajuudessa.

* 1. Käsittelytoimien kuvaus

Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän ja käsittelijän velvollisuudet ja oikeudet kuvataan sitoumuksessa, siihen liittyvässä dokumentaatiossa ja kunnan ohjeistuksessa sekä viimeistään sitoumuksen mukaisen palvelun alussa laadittavassa käsittelytoimien kuvauksessa.

Palveluntuottaja sitoutuu noudattamaan sitoumuksessa, dokumentaatiossa tai ohjeistuksessa olevia käsittelytoiminnan ehtoja ja kuvauksia.

* 1. Rekisteröidyn oikeudet

Palveluntuottaja ilmoittaa kunnalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä.

Palveluntuottaja avustaa kuntaa asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, jotta kunta pystyy täyttämään velvollisuutensa vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Pyynnöt voivat edellyttää esimerkiksi sitä, että palveluntuottaja avustaa rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen. Palveluntuottaja ylläpitää luetteloa rekisteröityjen henkilötietojen oikaisuista tai poistoista, ellei toisin sovita. Luettelo on luovutettava kunnalle tai kunnan määrittelemälle kolmannelle taholle kunnan sitä pyytäessä. Edellä mainitut toimenpiteet sisältyvät sitoumuksen kohteena olevaan palveluun, ellei muuta ole sovittu.

Palveluntuottajan on huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan automaattisesti irrottaa palveluntuottajan järjestelmästä siirrettäväksi toiseen järjestelmään.

* 1. Henkilötietojen luovutusta koskevat rajoitukset

Palveluntuottajalla on valmius asettaa ja hallinnoida henkilötietojen luovutuksia koskevia rajoituksia, joita voi johtua esimerkiksi turvakiellosta. Palveluntuottajan on pystyttävä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan kunnan vaatimalla tavalla. Rekisteröidyn henkilötietojen 5 rajoittaminen ei saa johtaa muiden rekisteröityjen henkilötietojen rajoittamiseen, elleivät palveluntuottaja ja kunta erikseen toisin sovi.

Palveluntuottajan on huolehdittava turvakiellon alaisten tietojen suojaamisesta sekä muiden mahdollisten tiedojen luovutusta koskevien rajoitusten noudattamisesta.

* 1. Auditointi

Palveluntuottaja sallii kunnan tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin. Auditointi voidaan suorittaa kerran vuodessa, ellei palveluntuottajan sitoumusrikkomuksesta tai lainsäädännöstä muuta johdu.

Auditointi on suoritettava siten, että palveluntuottajan muiden asiakkaiden tietosuoja ei vaarannu. Palveluntuottaja vastaa siitä, että palvelu ja siihen liittyvät tietojärjestelmät on auditoinnin suorittamiseksi dokumentoitu asianmukaisesti.

Kunta vastaa auditoinnin kustannuksista. Jos auditoinnissa havaitaan merkittäviä puutteita palveluntuottajan tietosuojasääntelyn tai sitoumuksen noudattamisessa, auditoinnin kustannuksista vastaa palveluntuottaja.

Palveluntuottajan on korjattava auditoinnissa havaitut puutteet viipymättä, viimeistään 30 vuorokauden kuluessa kunnan kirjallisesta ilmoituksesta. Olennaiset puutteet on korjattava heti.

* 1. Kunnan tarvitsemat tiedot ja vaikutusten arviointi

Palveluntuottaja saattaa kunnan saataville tämän pyynnöstä kaikki tiedot, jotka kunta tarvitsee rekisterinpitäjälle ja palveluntuottajalle säädettyjen velvollisuuksien noudattamisen osoittamista varten.

Palveluntuottaja sitoutuu tarvittaessa avustamaan kuntaa tietosuoja-asetuksen mukaisen tietosuojaa koskevan vaikutusten arvioinnin tekemisessä, mahdollisessa ennakkokuulemisessa ja tietosuojaa koskevan sertifioinnin hankkimisessa. Ellei näiden toimien ole sovittu sisältyvän sitoumuksen kohteena olevaan palveluun, palveluntuottajalla on oikeus laskuttaa kohtuulliset työkustannukset.

* 1. Tietosuojaseloste

Palveluntuottaja osallistuu kunnan pyynnöstä tietosuojaselosteen laatimiseen. Ellei näiden toimien ole sovittu sisältyvän sitoumuksen kohteena olevaan palveluun, palveluntuottajalla on oikeus laskuttaa kohtuulliset työkustannukset enintään sitoumuksessa sovituilla henkilötyöhinnoilla.

1. Tietosuojaa koskeva ohjeet

Palveluntuottaja noudattaa kunnan henkilötietojen käsittelyssä sitoumuksessa sovittuja ehtoja sekä kunnan kirjallisia ohjeita. Kunta vastaa ohjeiden ylläpidosta ja saatavuudesta. Palveluntuottaja ilmoittaa ilman aiheetonta viivytystä kunnalle, jos kunnan antamat ohjeet ovat puutteellisia tai jos palveluntuottaja epäilee niitä lainvastaisiksi.

Kunnalla on oikeus muuttaa, täydentää ja päivittää palveluntuottajalle antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Palveluntuottaja on oikeus laskuttaa muutosten toteuttamisesta kohtuulliset työkustannukset enintään sitoumuksessa sovituilla henkilötyöhinnoilla, mikäli muutosten toteuttamisesta aiheutuvat työmäärä ylittään yhden (1) henkilötyöpäivän. Jos ohjeiden muutoksista aiheutuu sitoumuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niistä sovitaan liitteen 12 kohdan mukaisesti.

1. Palveluhenkilöstö

Palveluntuottaja varmistaa, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä kunnan henkilötietoja, ovat sitoutuneet noudattamaan sitoumuksessa sovittuja salassapitoehtoja tai heitä koskee lakisääteinen salassapitovelvollisuus.

Palveluntuottaja varmistaa, että kaikki sen alaisuudessa toimivat henkilöt, joilla on pääsy kunnan henkilötietoihin, ovat tietoisia henkilötietojen käsittelyyn liittyvistä velvoitteistaan ja käsittelevät niitä ainoastaan sitoumuksen ja kunnan ohjeiden mukaisesti.

1. Alihankkijat ja ryhmittymä henkilötietojen käsittelijänä

Palveluntuottajan sitoumuksen ja tämän liitteen mukaisesti käyttämät alihankkijat, jotka osallistuvat kunnan henkilötietojen käsittelyyn, toimivat henkilötietojen käsittelijöinä kunnan puolesta ja lukuun.

Palveluntuottaja saa käyttää kunnan henkilötietojen käsittelyyn alihankkijan palveluita ilman kunnan etukäteen antamaa kirjallista lupaa. Sitoumuksen alkaessa käytettävät alihankkijat kuvataan liitteessä Käsittelytoimien kuvaus. Palveluntuottajan on tiedotettava kuntaa etukäteen kirjallisesti kaikista sellaisista muutoksista jotka koskevat henkilötietoja käsittelevien alihankkijoiden lisäämistä tai vaihtamista ja annettava kunnalle mahdollisuus vastustaa tällaisia muutoksia.

Palveluntuottajan on sovittava kirjallisesti kunnan alihankkijoiden henkilötietoja käsittelevien alihankkijoiden kanssa siitä, että ne sitoutuvat noudattamaan omalta osaltaan palveluntuottajalle asetettuja velvoitteita sekä kunnan antamia henkilötietojen käsittelyyn liittyviä ohjeita. Palveluntuottajan on varmistettava, että sitoumuksen mukainen kunnan auditointioikeus voidaan ulottaa alihankkijaan. Palveluntuottaja vastaa käyttämänsä alihankkijan osuudesta kuin omastaan.

Palveluntuottaja vastaa siitä, että alihankkija noudattaa omalta osaltaan henkilötietojen käsittelijälle asetettuja velvoitteita. Jos kunta perustellusti katsoo, että palveluntuottajan alihankkija ei täytä tietosuojavelvoitteitaan, kunnalla on oikeus vaatia palveluntuottajaa vaihtamaan alihankkijaa. Ryhmittymän ollessa palveluntuottajana, tämän liitteen velvoitteet koskevat kaikkia ryhmittymän jäseniä ja ryhmittymän jäsenten alihankkijoita, jotka osallistuvat kunnan henkilötietojen käsittelyyn.

1. Henkilötietojen käsittelyn paikka

Palveluntuottaja ei saa siirtää henkilötietoja EU:n tai ETA-alueen ulkopuolelle, ellei tästä erikseen sovita. Jos osapuolet sopivat, että palveluntuottajaa saa siirtää kunnan henkilötietoja EU:n tai Euroopan talousalueen, osapuolet huolehtivat siitä, että henkilötietojen siirto toteutetaan tietosuojasääntelyn ja kulloinkin voimassa olevien henkilötietojen siirtoa koskevien vaatimusten mukaisesti.

1. Tietoturvaloukkaukset

Palveluntuottajan on ilmoitettava kunnalle kirjallisesti tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja viimeistään 36 tunnin kuluessa. Ilmoitus on tehtävä osoitteella tietosuojavastaava@somero.fi. Lisäksi palveluntuottaja sitoutuu ilmoittamaan kunnalle muista palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Ilmoitus on tehtävä edellä mainitussa määräajassa, ellei sitoumuksessa tai se liitteissä ole sovittu lyhyemmästä määräajasta.

Palveluntuottajan on annettava kunnalle vähintään seuraavat tiedot tietoturvaloukkauksesta:

1) tapahtuneen tietoturvaloukkauksen kuvaus, mukaan lukien asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat tiedossa;

 2) tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;

 3) kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja

 4) kuvaus toimenpiteistä, joita palveluntuottaja ehdottaa tai joita se on jo toteuttanut tietoturvaloukkauksen johdosta, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Henkilötietojen tietoturvaloukkauksen havaittuaan palveluntuottaja ryhtyy viipymättä toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi. Tietoturvaloukkauksen sattuessa palveluntuottaja avustaa kuntaa tietosuoja-asetuksen 33 ja 34 artiklojen mukaisen ilmoituksen tekemisessä valvontaviranomaiselle ja rekisteröidylle.

1. Kunnan ilmoitukset ja reklamaatiot

Palveluntuottaja sitoutuu vastaamaan viimeistään 72 tunnin kuluessa kunnan yhteydenotosta kunnan tietosuojaa koskeviin ilmoituksiin, reklamaatioihin ja muihin viesteihin.

Tietosuoja-asetuksen tarkoittamista tietoturvaloukkauksista ilmoittamiseen sovelletaan kohdan 10. mukaisia määräaikoja ja menettelyä.

1. Sitoumuksen muuttaminen

Tietosuojaa koskeva lainsäädäntö on muutostilassa. Jos lainsäädäntöön tai sen tulkintaan ja sitä koskeviin määräyksiin, ohjeisiin ja suosituksiin tulee muutoksia, jotka vaikuttavat kunnan velvollisuuksiin tai vastuisiin, osapuolet voivat tarkentaa ja muuttaa tätä sitoumusta muutoksia vastaavalla tavalla. Muutoksista voi aiheutua palveluntuottajalle lisäkustannuksia.

Ellei sitoumuksessa ole toisin sovittu, palveluntuottajalla on oikeus laskuttaa kohtuulliset työkustannukset enintään sitoumuksessa sovituilla henkilötyöhinnoilla, mikäli lisäkustannuksia aiheutuu enemmän kuin yhtä (1) henkilötyömäärää vastaava määrä. Tällaisessa tapauksessa palveluntuottaja laatii kunnan hyväksyttäväksi tehtäväkohtaisen työmääräarvion ennen työn toteutusta.

1. Henkilötietojen käsittelyn päättyminen

Palveluntuottaja ei saa poistaa kunnan lukuun käsittelemiään henkilötietoja sitoumuskauden aikana ilman kunnan nimenomaista pyyntöä.

Sitoumuksen tai siihen liittyvän palveluntuottajan avustamisvelvollisuuden päättyessä palveluntuottaja palauttaa viipymättä kunnalle kaikki kunnan puolesta käsitellyt henkilötiedot jäsennellyssä, yleisesti käytettävässä ja koneluettavassa muodossa. Palveluntuottaja hävittää mahdolliset kopiot ja varmuuskopiot henkilötiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos EU sääntelyssä, lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että palveluntuottaja säilyttää henkilötiedot. Kunta voi antaa tarkempia ohjeita palveluntuottajalle.

1. Sitoumusrikkomukset ja vastuu

Jos palveluntuottaja laiminlyö tai rikkoo tätä sitoumusta, sovellettavaa tietosuojasääntelyä tai muuta lainsäädäntöä, palveluntuottajan korvausvastuu on määritelty sitoumuksen lisäksi sovellettavassa lainsäädännössä. Tietosuojaan liittyvä sitoumusrikkomus tulkitaan olennaiseksi sitoumusrikkomukseksi.

Jos osapuoli on maksanut rekisteröidylle korvauksen tietosuojasääntelyn rikkomisen johdosta aiheutuneesta vahingosta, on tällä osapuolella periä samaan tietojenkäsittelyyn osallistuneelta toiselta osapuolelta tämän vahingonkorvausvastuuta vastaava osuus rekisteröidylle maksetusta korvauksesta. Osapuolen vastuu rekisteröidylle aiheutuneesta vahingosta määräytyy tietosuoja-asetuksen 82 artiklan 4 kohdan tai muussa tietosuojalainsäädännössä olevan vastaavan määräyksen mukaan.

Mikäli kunnalle määrätään tietosuoja-asetuksen 83 artiklassa tarkoitettu hallinnollinen sakko ja sakon voidaan katsoa johtuneen palveluntuottajan puolella olevasta menettelystä tai laiminlyönnistä, palveluntuottajan on velvollinen korvaamaan kunnalle sakkoa vastaavan määrän.

Mahdolliset sitoumuksessa tai muualla sovitut vastuunrajoitukset eivät rajoita osapuolen oikeutta saada toiselta osapuolelta edellä mainitut korvaukset.

1. Sovellettava laki

Sitoumukseen sovelletaan Suomen lakia.

1. Sitoumuksen liitteet ja asiakirjojen soveltamisjärjestys

Sitoumus ja liitteet täydentävät toisiaan. Jos sitoumusasiakirjat ovat keskenään ristiriidassa, noudatetaan niitä seuraavassa järjestyksessä:

1. Sitoumus
2. Liite 1. Henkilötietojen käsittelytoimien kuvaus