Kaupunginkanslia
Oikeuspalvelut 25.11.2019

TIETOSUOJA- JA SALASSAPITOLIITE

HELSINGIN KAUPUNKI

Helsingin kaupunki	Postiosoite	Sähköposti	Puhelin	Faksi	Y-tunnus
Kaupunginkanslia	PL 1	oike@hel.fi	+358 9 310 1641	+358 9 310 36173	0201256-6
Oikeuspalvelut	00099 HELSINGIN KAUPUNKI				

Sisällys

A. JOHDANTO

1. Määritelmät

(1) **Alihankkija** tarkoittaa Sääntökirjan mukaisia Palveluntuottajan alihankkijoita.

(2) **Palvelu** tarkoittaa sitä palvelua, jonka toteuttajaksi Palvelunjärjestäjä on Palveluntuottajan hyväksynyt sähköisessä palvelusetelijärjestelmässä.

(3) **Sääntökirja** tarkoittaa palvelusetelipalvelujen tuottamisen sääntökirjan yleistä osaa sekä palvelukohtaisesti soveltuvia erityisiä osia.

(4) **Suojattava tieto** tarkoittaa kaikkea sellaista tietoa tiedon muodosta riippumatta, jonka Osapuoli on luovuttanut toiselle Osapuolelle, tai jonka Tilaaja on tallentanut Palveluun, tai joka on syntynyt Palvelun tuottamisessa, tai jonka Osapuoli on muuten saanut tietoonsa, ja

i. joka on määritelty salassa pidettäväksi viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999, jäljempänä ”julkisuuslaki”) tai muussa lainsäädännössä; tai
ii. kyseessä on sellaisen asiakirjan tieto, joka ei ole vielä tullut julkisuuslain tarkoittamalla tavalla julkiseksi; tai
iii. kyseessä on muu tieto, jonka Tilaaja on merkinnyt salassa pidettäväksi tai kuuluvan Suojattaviin tietoihin tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin; tai
iv. kyseessä on muu tieto, jonka Osapuolet ovat sopineet kuuluvan Suojattaviin tietoihin; tai
v. kyse on henkilötiedoista tai henkilörekisteristä.

(5) **Osapuolet** tarkoittaa Sääntökirjassa määriteltyjä **Palvelunjärjestäjää** ja **Palveluntuottajaa**.

(6) **Tietosuoja-asetus** tarkoittaa Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

(7) **Henkilötietojen käsittely** tarkoittaa Tietosuoja-asetuksen 4 artiklan mukaisesti 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, tietojen luovuttamista

siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

(8) **Tietosuoja- ja salassapitoliite** tarkoittaa tätä Sääntökirjan liitteenä olevaa asiakirjaa.

2. Yhteyshenkilöt

(1) Palvelunjärjestäjän yhteyshenkilö tietoturvallisuusasioissa:
Markku Havukainen. Yhteystiedot: markku.havukainen@hel.fi,
+358 (0) 40 487 9952 tai +358 (0) 9 310 75490.

(2) Palveluntuottajan yhteyshenkilö tietoturvallisuusasioissa:
Palveluntuottaja ilmoittaa Palvelunjärjestäjälle erikseen yhteyshenkilönsä tietoturvallisuusasioissa. Yhteyshenkilön tiedot on toimitettava osoitteeseen sote.tilaajavastuu@hel.fi.

(3) Osapuolet sitoutuvat ilmoittamaan välittömästi toisilleen tietoturvallisuusasioiden yhteyshenkilön vaihtumisesta.

3. Tietosuoja- ja salassapitoliitteen tausta ja tarkoitus

(1) Palvelunjärjestäjä velvoittaa Palveluntuottajan noudattamaan Sääntökirjan määräyksiä. Palvelun tuottamisesta noudatetaan sitä, mitä Sääntökirjassa on määrätty.

(2) Tässä Tietosuoja- ja salassapitoliitteessä määritellään Osapuolten välillä noudatettavat turvallisuusjärjestelyt ja Suojattavaa tietoa koskevat järjestelyt Sääntökirjan sisältämän Palvelun tuottamisessa sekä kaikessa Sääntökirjaan liittyvässä Osapuolten välisessä yhteistyössä.

(3) Osapuolet tiedostavat, että Sääntökirjan perusteella toimitettavaan Palveluun sisältyy sellaista tietoa, jonka salassa pysyminen voi olla mm. Palvelunjärjestäjän ja yksilöiden turvallisuuden ja oikeuksien, Palvelunjärjestäjän toiminnan, lainsäädännön asettamien oikeuksien ja velvollisuuksien sekä viranomaisia ja yksilöitä sitovien ohjeiden noudattamisen kannalta kriittistä. Tällä Tietosuoja- ja salassapitoliitteellä Osapuolet pyrkivät varmistamaan, että Suojattavat tiedot pysyvät salassa ja Palvelun tuottamisessa noudatetaan tietoturvallisuutta koskevaa lainsäädäntöä.

(4) Huolimatta siitä, mitä Sääntökirjassa tai muissa Osapuolten välisissä asiakirjoissa on mahdollisesti sovittu tämän Tietosuoja- ja salassapitoliitteen piiriin kuuluvista asioista tai niihin liittyvistä vastuista taikka asiakirjojen keskinäisestä pätevyysjärjestyksestä, tätä Tietosuoja- ja salassapitoliitettä sovelletaan aina ensisijaisesti tämän Tietosuoja- ja salassapitoliitteen piiriin kuuluvissa asioissa.

(5) Tämä Tietosuoja- ja salassapitoliite koskee vain palveluseteleillä tuotettua Palvelua.

4. Alihankinta

(1) Palveluntuottaja ei saa ilman Palvelunjärjestäjän antamaa kirjallista ennakkolupaa käyttää henkilötietojen käsittelyyn muita alihankkijoita kuin Palveluntuottajan hyväksynnän yhteydessä ilmoitettuja Alihankkijoita. Palveluntuottajan on ilman aiheetonta viivästystä tiedotettava Palvelunjärjestäjälle kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat henkilötietojen käsittelijöinä toimivien Alihankkijoiden lisäämistä tai vaihtamista.

(2) Palveluntuottajan tulee huolehtia siitä, että se pystyy noudattamaan tämän Tietosuoja- ja salassapitoliitteen ehtoja myös käyttäessään Alihankkijoita. Palveluntuottajan on tiedotettava Alihankkijalle tämän Tietosuoja- ja salassapitoliitteen mukaisista velvoitteista sekä siitä, että toiminnan saattamisesta Tietosuoja- ja salassapitoliitteen edellyttämälle tasolle saattaa aiheutua kustannuksia. Palvelunjärjestäjä ei vastaa näistä kustannuksista.

(3) Palveluntuottaja vastaa siitä, että sen Alihankkijat toimivat tämän Tietosuoja- ja salassapitoliitteen ehtojen mukaisesti. Palveluntuottaja vastaa Alihankkijoistaan samalla tavoin kuin omasta toiminnastaan. Palveluntuottaja vastaa siitä, että Palvelunjärjestäjän tämän liitteen mukainen Palvelunjärjestäjän tarkastusoikeus ulottuu myös Palveluntuottaja Alihankkijoihin.

(4) Palveluntuottaja vastaa siitä, että Alihankkijan työntekijät, jotka osallistuvat Palvelujen toimittamiseen Palvelunjärjestäjälle, ovat tietoisia ja sitoutuneita noudattamaan tämän Tietosuoja- ja salassapitoliitteen ehtoja.

(5) Tässä Tietosuoja- ja salassapitoliitteessä Palveluntuottaja henkilöstölle asetettavia velvoitteita sovelletaan myös Alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.

B. TIETOTURVALLISUUS JA SALASSAPITO

5. Osapuolten yleiset velvoitteet

(1) Palveluntuottaja ja sen Alihankkija noudattavat tätä Tietosuoja- ja salassapitoliitettä ja Palvelunjärjestäjän tietoturvallisuusohjeita Palvelun tuottamisessa. Lisäksi Palveluntuottaja ja sen Alihankkija noudattavat Palveluntuottajan sisäisiä tietoturvallisuusohjeita siltä osin, kuin ne eivät ole ristiriidassa Sääntökirjan, Sääntökirjan liitteiden, tämän Tietosuoja- ja salassapitoliitteen tai Palvelunjärjestäjän tietoturvallisuusohjeiden kanssa.

(2) Palvelunjärjestäjän tietoturvallisuusohjeet sisällytetään Palvelun dokumentaatioon. Ohjeiden muutoksista ja muutosten vaikutuksista Palvelun tuottamiseen sovitaan erikseen kirjallisesti.

(3) Palveluntuottaja vastaa siitä, ettei Palvelunjärjestäjän Suojattavien tietojen luottamuksellisuus, saatavuus tai eheys vaarannu Palveluntuottajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Tietosuoja- ja salassapitoliitteen tai Sääntökirjan vastaisen toiminnan johdosta.

(4) Palveluntuottaja vastaa siitä, että sen tuottama Palvelu on vikasietokykyinen ja Palveluun tallennetut tiedot pystytään palauttamaan nopeasti fyysisen tai teknisen vian sattuessa.

(5) Palvelunjärjestäjä vastaa siitä, että se noudattaa omassa toiminnassaan tätä Tietosuoja- ja salassapitoliitettä ja tietosuojaa koskevaa lainsäädäntöä ja pyrkii kaikin kohtuullisin keinoin myötävaikuttamaan Palvelunjärjestäjän mahdollisuuksiin toimia tämän liitteen mukaisesti.

(6) Palvelunjärjestäjä laatii tarvittaessa tietojärjestelmäselosteen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annetun asetuksen edellyttämällä tavalla.

6. Palveluntuottajan tietoturvallisuus

(1) Palveluntuottaja informoi Palvelunjärjestäjää Palvelun tietoturvallisuudesta ja muista vaatimustenmukaisuuteen liittyvistä seikoista pitämällä Palvelunjärjestäjään aktiivisesti yhteyttä ja siten, että Palveluntuottaja on niistä tietoinen.

(2) Palveluntuottaja sitoutuu toteuttamaan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet Suojattavien tietojen käsittelyn turvallisuuden varmistamiseksi ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tar-

koitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit sekä noudattamaan Palvelunjärjestäjän ohjeita ja mahdollisia Palvelunjärjestäjän ohjeiden päivityksiä.

(3) Palveluntuottaja määrittelee organisaatiossaan tietoturvallisuuteen liittyvät tehtävät ja vastuut sekä nimeää henkilöt Palveluun liittyvistä tietoturva-asioista tiedottamiseen ja tietoturvapoikkeamista raportointiin. Palveluntuottaja ulottaa vastaavan velvollisuuden myös Palvelun toimittamiseen liittyviin Alihankkijoihin.

(4) Palveluntuottaja vastaa siitä, että sen ja sen Alihankkijan henkilöstön käytettävissä on helposti saatavilla olevat ajantasaiset ja asianmukaiset tämän Tietosuoja- ja salassapitoliitteen mukaiset tietoturvaan ja tietosuojaan liittyvät ohjeistukset ja dokumentit.

(5) Tietoturvallisuuspäivityksien, käyttöoikeuksien valvonnan, käyttöoikeuksien hallinnan ja muiden vastaavien tietoturvallisuuteen liittyvien käytäntöjen osalta sovelletaan Sääntökirjassa tai Palvelunjärjestäjän tietoturvallisuusohjeissa määriteltyjä tai erikseen sovittuja käytäntöjä.

6.1 Henkilöstöturvallisuus ja turvallisuusselvitykset

(1) Palveluntuottaja ylläpitää ajantasaista listaa Palvelun tuottamiseen osallistuvien henkilöiden kulkuoikeuksista, pääsyoikeuksista ja käyttövaltuuksista.

(2) Palvelunjärjestäjä voi edellyttää turvallisuusselvityksistä annetussa laissa (726/2014) määritellyissä tilanteissa kyseisessä laissa tarkoitettua turvallisuusselvitystä tai tarvittaessa tasoltaan vastaavaa ulkomaista turvallisuusselvitystä Palvelun tuottamiseen osallistuvista Palveluntuottajan tai sen Alihankkijan työntekijöistä, jotka käsittelevät Suojattavia tietoja tai pääsevät järjestelmiin, jotka sisältävät Suojattavia tietoja.

(3) Turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta ja turvallisuusselvityksen teettämisestä vastaa Palveluntuottaja.

(4) Palvelunjärjestäjä vastaa edellä kuvattujen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Palveluntuottajan tai sen Alihankkijan henkilöstössä tapahtuu Palvelunjärjestäjästä riippumaton vaihdos tai lisäys, Palveluntuottaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.

6.2 Tietoaineistoturvallisuus

(1) Palveluntuottaja noudattaa julkisuuslaissa tarkoitettua hyvää tiedonhallintatapaa, hyvää tietojen käsittelytapaa, Tietosuoja-asetusta sekä muuta tietojen suojaamista ja tietosuojaa koskevaa lainsäädäntöä Palvelun tuottamisessa.

(2) Palvelunjärjestäjällä on oikeus luokitella Suojattavat tiedot niiden suojaustarpeen perusteella ja määritellä kullekin luokalle tietoturvallisuustaso ja sen mukaiset tietoturvatoimeenpiteet ja -ohjeet. Palveluntuottaja käsittelee Palvelunjärjestäjän Suojattavia tietoja Palvelunjärjestäjän luokitusten edellyttämällä tavalla.

6.3 Pääsy tiloihin

(1) Palveluntuottajan ja sen Alihankkijan sellaiset tilat, joissa säilytetään, käytetään tai muutoin käsitellään Suojattavia tietoja (jäljempänä Tilat), tulee olla asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi Tiloihin ja siellä oleviin Suojattaviin tietoihin.

(2) Mikäli Palvelua suoritetaan Palveluntuottajan tai sen Alihankkijan tiloissa, Palveluntuottajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. erityistilanteiden varalta. Osapuolet sopivat tarvittaessa Palveluun liittyvistä tarkemmista vaatimuksista.

(3) Henkilöt, joille ei ole myönnetty oikeutta Suojattaviin tietoihin tai niitä sisältäviin järjestelmiin kohdan 6.4 mukaisesti, saavat oleskella Tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Suojattavia tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

(4) Henkilöiden, joilla on pääsy Suojattaviin tietoihin, tulee olla tunnistettavissa kuvallisella henkilökortilla tai muulla vastaavalla tavalla.

6.4 Pääsy järjestelmiin ja tietoihin

(1) Palveluntuottaja vastaa siitä, että Suojattavia tietoja annetaan, sellaisia tietoja pääsee käsittelemään tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain nimetyille Palveluntuottajan ja sen Alihankkijan henkilöstöön kuuluville henkilöille, joille on annettu oikeus päästä kyseisiin järjestelmiin tai tietoihin, ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan.

(2) Palveluntuottaja vastaa siitä, että kohdassa 6.4(1) tarkoitetut henkilöt noudattavat tätä Tietosuoja- ja salassapitoliitettä.

(3) Palveluntuottaja vastaa siitä, että kohdassa 6.4(1) tarkoitettu henkilö on tehnyt kirjallisen, tämän Tietosuoja- ja salassapitoliitteen mukaisen salassapitositoumuksen ennen kuin hän aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin. Palvelunjärjestäjän pyynnöstä kyseinen salassapitositoumus on esitettävä Palvelunjärjestäjälle.

(4) Palveluntuottajan käyttöoikeudet Palvelunjärjestäjän järjestelmiin tarkastetaan säännöllisesti vähintään vuoden välein ja tarpeettomat tai liian laajat käyttöoikeudet poistetaan. Tarkastamisesta vastaa kunkin järjestelmän osalta se Osapuoli, joka ylläpitää ja hallinnoi kyseisen järjestelmän käyttöoikeuksia. Pääsääntöisesti käytetään vain käyttäjäkohtaisia tunnuksia. Yhteiskäyttöiset käyttäjätunnukset ovat sallittuja vain Palvelunjärjestäjän luvalla.

(5) Palvelunjärjestäjän organisaation mahdolliset ylläpito-oikeudet ja muut käyttöoikeudet tarkastetaan säännöllisesti yhteisesti sovitulla tavalla.

7. Tietoturvaloukkausten käsittely

(1) Palveluntuottaja ilmoittaa Palvelunjärjestäjälle Palveluun liittyvistä tietoturvapoikkeamista kirjallisesti välittömästi saatuaan ne tietoonsa. Ilmoitusvelvollisuus koskee ainakin toteutuneita tietovuotoja/-murtoja, tietomurron yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia sekä muita vastaavaa poikkeamia, jotka ovat omiaan nostamaan riskiä Palvelunjärjestäjän Suojattavien tietojen luottamuksellisuuden vaarantumiselle.

(2) Lisäksi Palveluntuottaja ilmoittaa Palvelunjärjestäjälle muista Palveluntuottajan tuottaman palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia Palvelunjärjestäjän Suojattavien tietojen luottamukselliselle käsittelylle tai sellaisten henkilöiden asemaan ja oikeuksiin, joiden henkilötietoja Palveluntuottaja käsittelee. Ilmoitus on tehtävä välittömästi Palveluntuottajan saatua niistä tiedon.

(3) Palveluntuottajan on annettava Palvelunjärjestäjälle vähintään seuraavat tiedot tietoturvaloukkauksesta:

- kuvattava tietoturvaloukkaus; mikäli kyseessä on henkilötietoihin kohdistunut tietoturvaloukkaus, kuvattava mahdollisuuksien mukaan myös asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

- ilmoitettava tietosuojavastaava tai muu vastuuhenkilö, jolta voi saada asiassa lisätietoja;

- kuvattava tietoturvaloukkauksen todennäköiset seuraukset; sekä

- kuvattava toimenpiteet, joita Palveluntuottaja ehdottaisi tai joita se on toteuttanut tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Mikäli kaikkia edellä mainittuja tietoja ei ole mahdollista toimittaa samanaikaisesti, voidaan tiedot toimittaa vaiheittain ilman aiheetonta viivytystä.

(4) Palveluntuottaja ohjeistaa henkilöstönsä ja Alihankkijansa Palvelujen tuottamiseen liittyvissä häiriötilanteissa toimimisen sekä niistä ilmoittamisen osalta.

(5) Palveluntuottaja huolehtii häiriötilanteiden hallinnasta Pääsopimuksen mukaisesti siten, että ongelman rajaus ja korjaus suoritetaan asianmukaisesti Sääntökirjan mukaisten tai yhteistesti sovittujen menettelytapojen mukaisesti.

(6) Palveluntuottaja on velvollinen auttamaan Palvelunjärjestäjää tietoturvapoikkeamiin liittyvien vahinkojen minimoinnissa.

(7) Rikos- ja väärinkäyttötapauksissa tai sellaisia epäiltäessä Palvelunjärjestäjä ja Palveluntuottaja pyrkivät olosuhteet ja lainsäädännön vaatimukset huomioon ottaen neuvottelemaan jatkotoimenpiteistä. Palveluntuottajalla on velvollisuus avustaa Palvelunjärjestäjää asian selvittämisessä viranomaistahojen kanssa.

8. Tietoturvallisuuteen liittyvä muutoshallinta ja kehittäminen

(1) Palveluihin kohdistuvissa muutoksissa toimitaan Sääntökirjassa määritellyn muutoshallintamenettelyn mukaisesti.

(2) Tietojärjestelmän tai Palvelujen muuttamista tai laajentamista koskevan suunnittelun alkuvaiheessa tarkistetaan tietoturvallisuuteen liittyvät vaatimukset. Palvelunjärjestäjä määrittelee kyseiset vaatimukset. Palveluntuottaja vastaa Palvelunjärjestäjän määrittelemien vaatimusten toteutuskelpoisen ratkaisun kuvaamisesta.

(3) Palveluntuottaja kehittää Palvelua jatkuvasti tietoturvallisuuteen liittyvien vaatimusten täyttämiseksi.

(4) Palveluntuottaja seuraa Palvelun kannalta olennaista tietoturvallisuuteen liittyvää kehitystä ja uutisointia. Palveluntuottaja varautuu ja reagoi aktiivisesti uusiin tietoturvallisuuteen liittyviin vaaratekijöihin ja uhkiin.

(5) Tämän Tietosuoja- ja salassapitoliitteen yhteyshenkilöt vastaavat tämän liitteen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan yhteyshenkilöiden kesken vähintään kahden vuoden välein.

(6) Tähän Tietosuoja- ja salassapitoliitteeseen tehtävien muutosten voimaantulo edellyttää molempien Osapuolten hyväksymistä. Tämän Tietosuoja- ja salassapitoliitteen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

9. Salassapito

(1) Osapuolet soveltavat tässä Tietosuoja- ja salassapitoliitteessä määriteltyjä turvallisuusjärjestelyitä aina Palveluntuottajan tai sen Alihankkijan käsitellessä Suojattavaa tietoa.

(2) Palvelunjärjestäjä noudattaa julkisyhteisönä julkisuuslaissa sekä muussa lainsäädännössä olevia salassapitoa, julkisuutta ja yksityisyydensuojaa koskevia säännöksiä. Tällä Tietosuoja- ja salassapitoliitteellä ei voida poiketa lainsäädännön Palvelunjärjestäjälle asettamista pakottavista velvoitteista.

(3) Palveluntuottajan tulee Palvelua tuottaessaan huomioida erityisesti seuraavien tietoturvallisuusvelvoitteita määrittävien säädösten vaikutus Palvelun tuottamiseen:

- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Tietosuojalaki (1050/2018)
- EU:n tietosuoja-asetus (EU 2016/679)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki yksityisyyden suojasta työelämässä (759/2004)

(4) Osapuolet pitävät salassa kaikki Suojattavat tiedot. Suojattavia tietoja ei saa käyttää omaksi tai toisen hyödyksi tai vahingoksi.

(5) Osapuolet säilyttävät ja käsittelevät Suojattavaa tietoa siten, että se pysyy vain niiden henkilöiden hallussa, joilla on oikeus Suojattavaan tietoon, eikä se joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

(6) Palveluntuottaja käsittelee Suojattavia tietoja vain Palvelun tuottamisen edellyttämässä laajuudessa. Palveluntuottaja antaa Suojattavia tietoja vain niille henkilöille, jotka tarvitsevat Suojattavia tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Palveluntuottaja sitoutuu antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Suojattavien tietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin.

(7) Palveluntuottaja vastaa henkilöstön salassapitositoumuksista kohdan 6.4(3) mukaisesti.

(8) Palvelunjärjestäjä päättää tiedon antamisesta asiakirjasta, joka on saatu Palvelunjärjestäjältä tai joka on laadittu Palvelunjärjestäjän toimeksiantotehtävää suoritettaessa.

(9) Pääsopimuksen päättyessä Palveluntuottaja ja sen Alihankkijat palauttavat Palvelunjärjestäjän Suojattavaa tietoa sisältävän aineiston ja muun Palvelunjärjestäjän osoittaman Palvelunjärjestäjälle kuuluvan aineiston sekä hävittävät taltioillaan olevan tietoaineiston ja kopiot. Palveluntuottaja vastaa siitä, että Palvelunjärjestäjän aineisto on erillään tai erotettavissa Palveluntuottaja muusta aineistosta. Aineistoa ei saa hävittää, mikäli Palvelunjärjestäjä, laki tai viranomaisten määräykset vaativat sen säilyttämistä. Tällöin Palvelunjärjestäjä ohjeistaa Palveluntuottajaa tarkemmin siitä, miten sen tulee menetellä.

(10) Salassapitovelvollisuus on voimassa myös sen jälkeen, kun Palvelun tarjoaminen on päättynyt.

C. HENKILÖTIETOJEN KÄSITTELY

10. Henkilötietojen käsittely

(1) Palvelunjärjestäjä on Tietosuoja-asetuksen mukaisten henkilötietojen rekisterinpitäjä ja vastaa näiden tietojen käsittelystä. Osapuolet ymmärtävät, että rekisterinpitäjänä Palvelunjärjestäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää Tietosuoja-asetuksen sekä muun kulloinkin voimassaolevan henkilötietojen käsittelyyn ja tietosuojaan liittyvän lainsäädännön vaatimukset, ja että käsittelyssä varmistetaan rekisteröidyn oikeuksien suojelu.

(2) Palveluntuottaja ja sen Alihankkijat ovat Tietosuoja-asetuksessa tarkoitettuja henkilötietojen käsittelijöitä. Palveluntuottaja on velvollinen noudattamaan kaikkia henkilötietojen käsittelijälle asetettuja Tietosuoja-asetuksen sekä muun kulloinkin voimassa olevan lainsäädännön velvoitteita sekä varmistamaan alihankintaa koskevissa sopimuksissa, että sen Alihankkijat noudattavat niitä.

(3) Osapuolet ovat sopineet Sääntökirjan mukaisessa käsittelytoimien kuvauksessa seuraavista asioista:

a. Käsittelyn kohde (mitä tietoja sopimus koskee) ja kesto (sopimuksen voimassaoloaika)
b. Käsittelyn luonne (millaisesta käsittelystä sovitaan, esim. tietojen kerääminen/tallentaminen) ja tarkoitus (miksi henkilötietoja käsitellään, mikä on sopimuksen mukainen tarkoitus henkilötietojen käsittelylle)
c. Henkilötietojen tyyppi (mitä henkilötietoja käsitellään, esim. nimi, osoitetiedot) ja rekisteröityjen ryhmät (keitä rekisterissä on, esim. asiakkaat / onko 9 art. mukaisia erityisiä henkilötietoryhmiä, joiden tietojen käsittelyyn tarvitaan erityisperuste)

(4) Palveluntuottaja käsittelee henkilötietoja Palvelunjärjestäjän toimeksiannosta vain siinä määrin kuin se on Palvelun tuottamiseksi tarpeen ja vain siihen saakka, kunnes Palvelun tarjoaminen on päättynyt tai Palveluntuottajan avustamisvelvollisuus on päättynyt Palvelunjärjestäjän ohjeistuksen mukaisesti. Palveluntuottajalla ei ole oikeutta käyttää saamiaan henkilötietoja omassa toiminnassaan, käsitellä niitä tämän Tietosuoja- ja salassapitoliitteen vastaisesti, yhdistää henkilötietoja muuhun hallussaan olevaan aineistoon eikä luovuttaa niitä. Palvelunjärjestäjä ohjeistaa Palveluntuottajaa henkilötietojen siirtoon tai tuhoamiseen liittyvästä menettelystä Palvelun tarjoamisen päättymisen yhteydessä.

(5) Palveluntuottaja ei saa käsitellä, siirtää tai luovuttaa Palvelunjärjestäjän henkilötietoja EU tai ETA-alueen ulkopuolelle. Myös palvelimien tulee sijaita EU- tai ETA-alueella ja Palveluntuottajan tulee ilmoittaa Palvelunjärjestäjälle niiden sijoituspaikat. Palveluntuottajan on ilmoitettava Palvelunjärjestäjälle etukäteen, jos palvelimien sijaintipaikka muuttuu.

(6) Mikäli Palveluntuottaja käsittelee henkilötietoja omassaan tai Alihankkijansa järjestelmässä, ja mikäli rekisteröidyllä on oikeus saada tiedot koneellisessa muodossa, Palveluntuottajan on huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan automaattisesti irrottaa järjestelmästä siirrettäväksi toiseen järjestelmään.

(7) Mikäli Palveluntuottaja käsittelee henkilötietoja omassaan tai Alihankkijansa järjestelmässä, Palveluntuottaja on velvollinen tallentamaan lokitiedot kaikista henkilötietojen käsittelytoimista, mukaan lukien henkilötietojen katselusta. Palvelunjärjestäjän pyynnöstä Palveluntuottaja antaa kyseiset lokitiedot Palvelunjärjestäjälle. Lokitietoihin liittyvistä velvoitteista voidaan määrätä tarkemmin Sääntökirjassa tai sen liitteissä.

(8) Palvelunjärjestäjän, Palveluntuottajan ja Palveluntuottajan Alihankkijan on pyynnöstä tehtävä Tietosuoja-asetuksen 31 artiklan mukaisesti yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

(9) Palveluntuottajan on tarvittaessa avustettava Palvelunjärjestäjää Tietosuoja-asetuksen 35 artiklan mukaisen vaikutusten arvioinnin tekemisessä ja 36 artiklan mukaisen ennakkokuulemisen toteuttamisessa.

(10) Osapuolet laativat yhdessä Tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarviointidokumentin Palvelulle sen suunnitteluvaiheessa, mikäli sellainen on lainsäädännön tai viranomaisten ohjeistuksen mukaan laadittava.

(11) Mikäli Tietosuoja-asetus edellyttää tietosuojavastaavan nimeämistä, Palveluntuottajan on nimettävä Tietosuoja-asetuksen 37 artiklan mukaisesti tietosuojavastaava ja ilmoitettava hänen yhteystietonsa Palvelunjärjestäjälle. Tietosuojavastaava tai muu Palvelun tietoturvallisuudesta vastaava henkilö on velvollinen osallistumaan ilman eri veloitusta pyydettäessä Palvelun seurannan johtoryhmän tai muun vastaavan elimen kokouksiin.

(12) Palveluntuottajan tulee noudattaa sisäänrakennettua ja oletusarvoista tietosuojaa Palvelun toimittamisessa ja kehittämisessä. Tämä tarkoittaa tietosuojaperiaatteiden sisällyttämistä aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata henkilötietojen käsittelyn koko elinkaaren ajan.

(13) Palveluntuottaja sitoutuu ilman aiheetonta viivästystä ilmoittamaan Palvelunjärjestäjälle kaikista rekisteröityjen pyynnöistä, jotka koskevat Tietosuoja-asetuksen sekä muun voimassaolevan lainsäädännön mukaisten rekisteröidyn oikeuksien käyttämistä.

(14) Palveluntuottaja sitoutuu avustamaan Palvelunjärjestäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, jotta Palvelunjärjestäjä pystyy täyttämään velvollisuutensa vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Henkilötietojen käsittelijänä Palveluntuottaja ymmärtää, että näiden oikeuksien käyttämistä koskevat pyynnöt voivat edellyttää siltä avustamista rekis-

teröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa ja/tai henkilötietojen siirtämisessä järjestelmästä toiseen.

(15) Tietoturvaloukkauksen sattuessa Palveluntuottajan tulee avustaa Palvelunjärjestäjää Tietosuoja-asetuksen 33 ja 34 artiklojen edellyttämän ilmoituksen tekemisessä valvontaviranomaiselle ja rekisteröidylle.

(16) Mikäli Palveluntuottaja käsittelee luonnollisten henkilöiden osoite- ja muita yhteystietoja omassa tai Alihankkijansa järjestelmässä, Palveluntuottajalla on oltava valmius asettaa ja hallinnoida tietojen luovutuksia koskevia rajoituksia, jollaisia voi aiheutua esimerkiksi väestötietolain mukaisesta rekisteröidyn turvakiellosta. Palveluntuottajan tulee pystyä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan Palvelunjärjestäjän vaatimalla tavalla. Rekisteröidyn henkilötietojen rajoittaminen ei saa johtaa muiden rekisterissä olevien luonnollisten henkilöiden henkilötietojen rajoittamiseen, ellei Palvelunjärjestäjän ja Palveluntuottajan kesken kirjallisesti toisin sovita.

D. MUUT EHDOT

11. Palvelun seuranta ja tarkastaminen

(1) Tämän Tietosuoja- ja salassapitoliitteen mukaisen Palvelun seurannan ja tarkastamisen tavoitteena on Palvelun ylläpidon ja tietoturvallisuuden sekä niiden jatkuvan kehittämisen varmistaminen sekä Suojattavan tiedon salassapidon toteutuminen.

(2) Palvelunjärjestäjällä on oikeus muuttaa, täydentää ja päivittää Palveluntuottajalle antamiaan Tietoturvallisuusohjeita. Ohjeiden muutokset, täydennykset ja päivitykset voivat liittyä teknisiin tai organisatorisiin toimenpiteisiin, jotka koskevat tietoturvaa, henkilötietojen käsittelyä tai tietosuojaa. Palveluntuottaja tekee tarvittavat muutostyöt Palvelunjärjestäjän ohjeiden mukaisesti.

(3) Palveluntuottaja toimittaa Palvelunjärjestäjälle jälkikäteen tietoturvaraportin, josta tulee ilmetä ainakin:
   a. Mahdolliset henkilöstön ja alihankintaketjun muutokset ja tarvittaessa niihin liittyvät turvallisuusselvitykset
   b. Tietoturvallisuusohjeiden päivitystarvetta mahdollisesti aiheuttavat tuotekehityssuunnitelmat
   c. Muutokset tietoturva ja -suojaohjeistuksessa
   d. Tehdyt tietoturvallisuustoimet (haavoittuvuuksien paikkaukset, versiopäivitykset, turvaohjelmistojen asennukset jne.)

e. Toteutuneet tietovuodot/-murrot sekä niiden laajuus ja vakavuus. Henkilötietoja mahdollisesti vaarantavat vuodot Palveluntuottaja raportoi välittömästi.
f. Tietomurron yritykset
g. Paikkaamattomat järjestelmähaavoittuvuudet sekä muut vastaavat poikkeamat, jotka ovat omiaan nostamaan riskiä Palvelunjärjestäjän Suojattavien tietojen luottamuksellisuuden vaarantumiselle.

(4) Palveluntuottaja sitoutuu reagoimaan viimeistään 72 tunnin kuluessa Palvelunjärjestäjän yhteydenotosta ja vastaamaan viimeistään yhden (1) viikon kuluessa Palvelunjärjestäjän tietoturvaa, henkilötietojen käsittelyä tai tietosuojaa koskeviin ilmoituksiin, reklamaatioihin tai muihin viesteihin, pois lukien Tietosuoja-asetuksen mukaiset tietoturvaloukkaukset, joihin Palveluntuottaja reagoi kohdan 7 (1) mukaisesti välittömästi saatuaan ne tietoonsa.

(5) Palveluntuottaja seuraa tämän Tietosuoja- ja salassapitoliitteen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Palvelunjärjestäjälle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Palvelunjärjestäjä seuraa Palvelun turvallisuustason toteutumista yhteistyössä Palveluntuottajan kanssa.

(6) Palvelun tarkastamiseksi suoritettava auditointimenettely on määritelty tämän Tietosuoja- ja salassapitoliitteen kohdassa 12.

(7) Palvelunjärjestäjä ei vastaa Palvelun seurannan ja tarkastamisen perusteella tehtävistä korjauksista aiheutuvista kustannuksista.

12. Auditointi

(1) Palvelunjärjestäjällä on oikeus auditoida Palvelu ja sen toimittaminen sekä siihen liittyvät Palveluntuottajan järjestelmät. Auditoinnissa Palvelunjärjestäjällä on oikeus käyttää ulkopuolista auditoijaa.

(2) Auditointi on suoritettava siten, ettei Palveluntuottajan muiden asiakkaiden tietoturva tai heidän tietojensa luottamuksellisuus vaarannu.

(3) Palvelunjärjestäjä voi suorittaa auditoinnin enintään kaksi kertaa kalenterivuodessa, ellei pakottavasta lainsäädännöstä, viranomaismääräyksistä tai tietoturvauhasta muuta johdu. Tilaajalla on aina erityisestä syystä, kuten epäiltyjen tai toteutuneiden tietoturvapoikkeamien tai väärinkäytösten yhteydessä, oikeus suorittaa auditointi.

(4) Palveluntuottaja vastaa siitä, että Palvelu ja siihen liittyvät tietojärjestelmät on auditoinnin suorittamiseksi dokumentoitu asianmukaisesti.

(5) Palvelunjärjestäjä laatii ennen auditointiin ryhtymistä auditointisuunnitelman. Auditoija laatii auditointiraportin, johon sisältyy mahdollisten todettujen puutteiden lisäksi ehdotus tarvittavista korjaustoimenpiteistä. Palvelunjärjestäjä luovuttaa auditoijan laatiman tarkastusraportin Palveluntuottajalle korjaustoimenpiteitä varten.

(6) Palvelunjärjestäjä vastaa auditoinnin järjestämisen kustannuksista. Mikäli kuitenkin auditoinnissa havaitaan merkittäviä puutteita Toimittajan turvallisuusjärjestelyissä tai tämän Tietosuoja- ja salassapitoliitteen noudattamisessa, vastaa auditoinnin kustannuksista Palveluntuottaja.

(7) Palveluntuottajan tulee korjata tarkastuksessa havaitut puutteet viipymättä, kuitenkin viimeistään 30 vuorokauden kuluessa Palvelunjärjestäjän kirjallisesta ilmoituksesta, ellei asiasta ole toisin nimenomaisesti sovittu. Olennaiset puutteet, jotka muodostavat ilmeisen uhan tietoturvallisuudelle, on korjattava heti.

(8) Palveluntuottajan Sääntökirjan tai tämän Tietosuoja- ja salassapitoliitteen vastaisista laiminlyönneistä tai virheistä aiheutuneet auditoinnissa ilmenneet puutteet ja virheet Palveluntuottaja korjaa veloituksetta.

(9) Palvelunjärjestäjällä on oikeus luovuttaa muille viranomaisille tieto tarkastuksen lopputuloksesta.

13. Vahingonkorvaus ja seuraamukset

(1) Jos Palvelunjärjestäjä on Tietosuoja-asetuksen 82 artiklan 4 kohdan mukaisesti maksanut rekisteröidylle korvauksen aiheutuneesta vahingosta, ja jos kyseisen vahingon voidaan katsoa aiheutuneen Palveluntuottajan tai sen palveluksessa olevan henkilön tai Palveluntuottajan Alihankkijan menettelyn tai laiminlyönnin seurauksena tai johdosta, on Palveluntuottaja velvollinen korvaamaan Palvelunjärjestäjälle Palvelunjärjestäjän maksaman korvauksen täysimääräisesti sovittujen vastuunrajoitusten estämättä.

(2) Mikäli Sääntökirjan tai Tietosuoja- ja salassapitoliitteen velvoitteita ei noudateta, on Palvelunjärjestäjällä oikeus peruuttaa Palveluntuottajan hyväksyminen ja poistaa Palveluntuottajan nimi hyväksyttyjen Palveluntuottajien listasta välittömästi.

14. Tietosuoja- ja salassapitoliitteen voimassaolo

(1) Tämä Tietosuoja- ja salassapitoliite astuu voimaan, kun Palveluntuottaja hyväksytään palvelusetelillä hankittavien ja toteutettavien sosiaali- ja terveyspalvelujen tuottajaksi ja on voimassa niin kauan kuin Palveluntuottaja tuottaa Palvelua.