



Vantaan ja Keravan hyvinvointialue

Tietoturvallisuussopimus

Liite 1 Tietoturvallisuussopimus

Liite 1.1 Salassapito- ja tietoturvasitoumus



Liite 1.1 Salassapito-
ja tietoturvasitoumus.docx

Liite 1.2 Henkilötietojen käsittelyn vaatimukset



Liite 1.2
Henkilötietojen käsitte

Liite 1.3 Henkilötietojen kuvaus / seloste käsittelytoimista



Liite 1.3
Henkilötietojen kuvaus

Liite 1.4 Henkilötietojen tietoturvaloukkausten selvittäminen



Liite 1.4
Henkilötietojen tietotu

Liite 1.5 Yhteyshenkilöt



Liite 1.5
Yhteyshenkilöt.docx



Sisällysluettelo

1 Sopimuksen osapuolet	1
2 Määritelmät	2
3 Sopimuksen tausta	2
4 Sopimuksen kohde	3
5 Tietoturva	3
6 Tietosuoja	4
7 Lokitiedot	6
7.1 Tiedonhallintalain mukaiset lokitiedot	6
7.2 Asiakas- ja hyvinvointitietojen käsittelyn ja luovutuksen lokitiedot	6
7.3 Tekniset lokit sekä tietoturvan audit trail -loki	7
7.4 Lokitietojen säilyttäminen	8
7.5 Muut lokitietoja koskevat velvoitteet	8
8 Turvallisuusselvitykset	9
9 Salassapito	9
10 Henkilöstö	10
11 Tietosuojaa ja tietoturvaa koskeva auditointi	11
12 Korvausvastuu ja vastuunrajoitukset	11
13 Muut ehdot	11
14 Voimaan jäävät ehdot	12
15 Sopimuksen voimaantulo	12
16 Sopimuksen voimassaolo	12
17 Sopimusasiakirjat ja soveltamisjärjestys	12
18 Sopimuskappaleet ja allekirjoitukset	12

1 Sopimuksen osapuolet

Tilaaaja: Vantaan ja Keravan hyvinvointialue (Myöhemmin "Tilaaaja" tai "Osapuoli")
Y-tunnus: 3221356-1
Osoite: PL 1000, 01088 Vantaan ja Keravan hyvinvointialue

Toimittaja: Samaria Rf
Y-tunnus: 0130415-3
Osoite: Asentajantie 12, 06150 Porvoo

Yhdessä myös "Sopijapuolet".



2 Määritelmät

Henkilötietojen tietoturvaloukkaus, Personal Data Breach: Tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. vrt. **Tietoturvaloukkaus**

Palvelut: Pääsopimuksen kohteena olevat palvelut.

Pääsopimus: Määritelty Sopimuksen luvussa 3.

Sopimus: Tämä sopimus.

Tietosuoja-lainsäädäntö: tarkoittaa, rajoituksetta ja soveltuvin osin, kaikkea kulloinkin voimassa olevaa henkilötietojen suojaan liittyvää EU-lainsäädäntöä ja kansallista lainsäädäntöä, kuten EU:n yleistä tietosuoja-asetusta (2016/679) sekä kansallista tietosuojalakia (1050/2018).

Tietoturvatapahtuma, Information Security Event, Anomaly: yksittäinen tapahtuma, joka saattaa vaikuttaa tietoturvaan

Tietoturvapoikkeama, tietoturvahäiriö, Information Security Incident: yksi tai useampi tietoturvatapahtuma, vaarantaen tietoturvan ja vaikuttaen organisaation toimintaan

Tietoturvaloukkaus, Information Security Breach: oikeudeton puuttuminen tietoon. vrt. **Henkilötietojen tietoturvaloukkaus**

Sopimukseen sovelletaan lisäksi EU:n yleisen tietosuoja-asetuksen (2016/679, myös GDPR) ja Pääsopimuksen määritelmiä.

3 Sopimuksen tausta

Tämä Sopimus on liitesopimus alla mainittuun sopimukseen.

Mielenterveys- ja päihdekuntoutujien asumispalvelujen hankinta

Edellä mainittu sopimus myös Pääsopimus VAKEDno-2025-2937.

Sopimus koskee koko Vantaan ja Keravan hyvinvointialueen organisaatiota sellaisena kuin se kulloinkin julkisyhteisönä on määritelty.

Mikäli Pääsopimukseen sovelletaan JIT 2015 Yleisiä ehtoja, Sopimusta sovelletaan kyseisten ehtojen kohdan 18 sijaan. Mikäli Pääsopimukseen sovelletaan JIT 2015 Palvelut verkon kautta -ehtoja, Sopimusta sovelletaan kyseisten ehtojen kohtien 13 ja 14 sijaan.

Mikäli Pääsopimukseen sovelletaan Julkisten hankintojen yleisiä sopimusehtoja palveluhankinnoissa (JYSE Palvelut 2014, myöhempine muutoksineen), Sopimusta sovelletaan kyseisten ehtojen kohdan 21 sijaan.



Mikäli Pääsopimukseen sovelletaan Julkisten hankintojen yleisiä sopimusehtoja tavarahankinnoissa (JYSE Tavarat 2014, myöhemmine muutoksineen), Sopimusta sovelletaan kyseisten ehtojen kohdan 17 sijaan.

4 Sopimuksen kohde

Sopimuksen kohteena on Tilaajan ja Toimittajan välisen voimassa olevan Pääsopimuksen kohteen mukaisen Palvelun tietosuoja- ja tietoturvaehdot siltä osin kuin Sopimuksessa on sovittu.

Sopijapuolet yhdessä täyttävät yhdessä liitteen 1.3 (liite 1.3 Henkilötietojen kuvaus / seloste käsittelytoimista). Sopijapuolet vastaavat omista kustannuksistaan, jotka liittyvät edellä mainittuun selvitystyöhön.

Mikäli Sopimuksen piiriin kuuluvat tehtävät aiheuttavat Toimittajalle muutostöitä, joita ei ole huomioitu alkuperäisessä tarjouspyynnössä, Toimittaja tekee niistä työmääräarvion ja tarjouksen. Tilaaja tekee muutoksista erikseen hankintapäätöksen, jonka perusteella muutostyö tilataan.

Tilaaja voi myös päätöksellään keskeyttää tai lopettaa Palvelujen käytön kokonaan tai osittain väliaikaisesti ilman, että se tulkitaan sopimusrikkomukseksi, jos ilmenee vakavia tietosuoja- tai tietoturva- puutteita. Tilaaja jatkaa Palvelujen käyttöä, kun tietosuoja- tai tietoturva- puutteet on korjattu. Osapuolet ymmärtävät, ettei Toimittajalla ole oikeutta veloittaa Palvelujen käytöstä siltä osin, kuin Tilaaja on päätöksellään keskeyttänyt tai lopettanut Palvelujen käytön.

Sopijapuolten sopimus-, tietosuoja-, tietoturva- ja yhteyshenkilöt on kuvattu Pääsopimuksessa [tai tämän Sopimuksen liitteessä 1.5]. Yhteyshenkilöiden tehtävänä on seurata ja valvoa oman vastuualueensa osalta Sopimuksen toteutumista ja tiedottaa oman organisaationsa sisällä ja toisen Sopijapuolen yhteyshenkilölle Sopimuksen toteutumiseen liittyvistä asioista. Yhteyshenkilöiden vaihtumisesta on ilmoitettava kirjallisesti viipymättä toisen Sopijapuolen sopimusyhteyshenkilölle.

Mikäli Pääsopimukseen sovelletaan JIT 2015 Yleisiä ehtoja, Sopimusta sovelletaan kyseisten ehtojen kohdan 18 sijaan. Mikäli Pääsopimukseen sovelletaan JIT 2015 Palvelut verkon kautta -ehtoja, tätä Tietosuoja- ja salassapitoliiettä sovelletaan kyseisten ehtojen kohtien 13 ja 14 sijaan.

5 Tietoturva

Toimittaja huolehtii käsittelemiensä tietojen asianmukaisesta suojaamisesta laittoman tai tapaturmaisen häviämisen tai hävittämisen varalta.

Toimittaja huolehtii siitä, että sen sopimusvelvoitteiden täyttämässä mahdollisesti käyttämät tietotekniset laitteet sekä palvelutuotannon tilat on asianmukaisesti suojattu tietoturvariskejä vastaan ja että suojaukseen ja tiedonvarmistukseen liittyviä menettelyjä noudatetaan. Tilaajan on huolehdittava vastaavin tavoin omista tietoteknisistä laitteistaan ja tiloistaan.

Toimittajan velvollisuutena on huolehtia tietojen varmuuskopioinnista, varmuuskopioiden toimivuuden tarkastamisesta ja tarvittaessa niiden palauttamisesta. Varmistukset tulee ottaa päivä-, kuukausi- ja vuosikierrolla, ellei erikseen toisin sovita. Varmistuskopioita tulee säilyttää vähintään Sopimuksen voimassaoloajan, ellei laissa tai Pääsopimuksessa toisin edellytetä. Toimittaja on velvollinen puolivuositain, ellei toisin erikseen sovita, todentamaan kirjallisesti Tilaajalle, että varmistuskopiointi on onnistunut ja tietojen eheys on säilynyt sekä myös tietojen palautus onnistuu.



Toimittaja vastaa Tilaajan tietojen tai tiedostojen tuhoutumisesta, katoamisesta tai muuttumisesta ja tästä aiheutuneista välittömistä kuluista, kuten tietojen ja tiedostojen uudelleen luomisen aiheuttamista kustannuksista niiltä osin kuin se on velvollinen ottamaan edellä mainitut varmistukset. Toimittajalla ei ole edellä mainittua vastuuta, mikäli Tilaaja tai Tilaajan vastuulla oleva aiheuttaa omalla toiminnallaan tietojen tai tiedostojen katoamisen taikka häviämisen taikka mikäli tietojen tai tiedostojen katoaminen aiheutuu Toimittajan vaikutusvallan ulkopuolella olevasta seikasta. Selvyden vuoksi todetaan kuitenkin, että Toimittaja on kuitenkin viimeksi mainitussa tapauksessa velvollinen erillistä korvausta vastaan palauttamaan Tilaajan tiedot ja auttamaan Tilaajaa tietojen ajantasaistamisessa.

Toimittaja on velvollinen pyydettyäessä sopimuskauden aikana toimittamaan selvityksensä omasta tietoturvan hallinnasta. Edellä mainitusta selvityksestä on vähintään käytävä ilmi alla mainitut asiat:

- Toimittajan tietoturva- ja tietosuojapolitiikka,
- Toimittajan tietoturvasertifioinnit
- Toimittajan asiakkaiden käyttäjätunnusten hallinnan periaatteet,
- Toimittajan lokienhallinnan periaatteet,
- Toimittajan varmistusten hallinnan periaatteet,
- Toimittajan toipumissuunnitelma
- Toimittajan tietoturvapäivitysten hallinta sekä
- Toimittajan suunnitelma ja menettelytavat Tietoturvaloukkausten varalle sekä
- Palvelun arkkitehtikuvauksen, josta ilmenee Palvelun rakenne, tietoliikennevaatimukset sekä tietovirrat.

Selvyden vuoksi todetaan, että kaikki edellä mainittu koskee myös Toimittajan käyttämiä alihankkijoita ja kolmansia osapuolia ja selvityksestä tulee ilmetä heidän osuutensa Toimittajan toimittamien Palvelujen tietoturvasta.

Toimittaja toimittaa ennen Sopimuksen allekirjoittamista edellä kuvatun selvityksen ja suunnitelman Tilaajalle tiedoksi, ellei erikseen toisin sovita.

6 Tietosuoja

Toimittajan tulee kaikessa Pääsopimuksen mukaisten velvoitteidensa täyttämässä noudattaa voimassa olevaa Tietosuojalainsäädäntöä.

Toimittaja vastaa siitä, että Pääsopimuksen mukainen Palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön vaatimusten mukainen, ottaen erityisesti huomioon tietojärjestelmien oletusarvoisen ja sisäänrakennetun tietosuojan periaatteet. Toimittaja huolehtii käsittelemiensä tietojen asianmukaisesta suojaamisesta varmistaakseen Tilaajan aineiston luottamuksellisuuden, eheyden ja saatavuuden.

Selvyden vuoksi todetaan, että tämän Sopimuksen luvun säännösten lähtökohtana on se, että Tilaajaa pidetään EU:n yleisen tietosuoja-asetuksessa rekisterinpitäjänä ja Toimittajaa henkilötietojen käsitteijänä.

Toimittajalla on oikeus käsitellä Tilaajan aineistoon sisältyviä Henkilötietoja:

- vain Pääsopimuksessa mainitulla perusteella tai Tilaajan kirjallisesti etukäteen antamalla luvalla,



- vain siinä määrin ja niin kauan, kuin se on Pääsopimuksen kohteen toteuttamiseksi välttämätöntä sekä
- vain tämän Sopimuksen ja Pääsopimuksen sekä Tilaaajan erikseen antamien dokumentoitujen ohjeiden mukaisesti.

Toimittaja saa käyttää Tilaaajan aineistoa Pääsopimuksen kohteen toteuttamiseen ja vain Pääsopimuksen kohteen toteuttamisen edellyttämässä laajuudessa. Toimittajan tulee huolehtia siitä, että Tilaaajan aineistoa käsittelevät vain ne Toimittajan lukuun työskentelevät henkilöt, joiden työtehtäviin Tilaaajan aineiston käsittely kuuluu.

Henkilötietojen käsittelyn käsittelyperuste on yksilöity Sopimuksen liitteessä 1.3.

Sopijapuolet ymmärtävät, että Toimittajalla ei ole oikeutta käyttää sellaisia Henkilötietoja, joista Tilaaaja vastaa rekisterinpitäjänä, mihinkään muuhun tarkoitukseen kuin Pääsopimuksen mukaisten velvollisuuksien täyttämistä varten.

Selvyyden vuoksi todetaan, että henkilötietojen luovuttaminen ja käsittely suoramainontaa, etämyyntiä ja muuta suoramarkkinointia varten on kielletty.

EU:n yleisen tietosuoja-asetuksessa määritellyistä henkilötietojen tietoturvaloukkauksista Sopijapuolen tulee raportoida toiselle Sopijapuolelle Pääsopimuksen liitteen 1.2 mukaisesti. Henkilötietojen tietoturvaloukkausta koskevan ilmoituksen tarkka sisältö on kuvattu Pääsopimuksen liitteessä 1.2 (Henkilötietojen käsittelyn vaatimukset) kohdassa 9 ja menettelyprosessi on kuvattu tämän Pääsopimuksen liitteessä 1.4. Toimittajalla ei ole oikeutta veloittaa tästä erikseen.

Mikäli Sopijapuoli laiminlyö tai rikkoo tässä henkilötietojen käsittelyä koskevassa lainsäädännössä tai EU:n yleisessä tietosuoja-asetuksessa määriteltyjä toimintavelvoitteita, määräyksiä, vastuita tai rajoitteita ja siitä aiheutuu seuraamuksia tai vahinkoa rekisteröidylle, Sopijapuolten vastuut määräytyvät EU:n yleisen tietosuoja-asetuksen mukaisesti.

Mikäli Toimittaja laiminlyö tai rikkoo Sopimuksessa määriteltyjä henkilötietojen käsittelyä koskevia toimintavelvoitteita, määräyksiä, vastuita tai rajoitteita ja siitä aiheutuu seuraamuksia tai vahinkoa Tilaaajalle, rekisteröidylle tai kolmannelle osapuolelle, Toimittaja vastaa vahinkojen korvaamisesta Pääsopimuksen mukaisesti.

Mikäli Tilaaaja joutuu oikeudellisesti puolustautumaan tietoturva- tai tietosuojaloukkausta vastaan, Toimittajan on toimitettava ilman aiheetonta viivytystä Tilaaajan käyttöön kaikki hallussaan oleva asiaan liittyvä aineisto sekä avustamaan Tilaaajaa puolustautumistoimenpiteissä. Aineisto on toimitettava ilman erillistä korvausta mutta avustamisesta Toimittajan on oikeus periä kohtuulliset kustannukset Pääsopimuksessa annettujen hintojen perusteella. Mikäli tietoturvaloukkaus johtuu Toimittajan toiminnasta, Toimittajan on viipymättä toimitettava kirjallinen selvitys tapahtumasta.

Toimittaja huolehtii omien tiedostojensa ja saamiensa kopiokappaleiden tuhoamisesta ja Toimittajan on todennettava tämä. Pääsopimuksen tai Henkilötietojen käsittelytarkoituksen päätyttyä Toimittajalle ei jää Tilaaajan henkilöstön tai asiakkaiden henkilötietoja, ellei lainsäädännöstä muuta johdu.

Sopimuksen liitteessä 1.2 on kuvattu henkilötietojen käsittelyä koskevat tarkemmat vaatimukset, joita Toimittaja ja sen alihankkijat, jotka käsittelevät henkilötietoja Tilaaajan puolesta ja lukuun, sitoutuvat noudattamaan.



7 Lokitiedot

Tässä luvussa 7 Järjestelmästä mainittu koskee Pääsopimuksen mukaista Ratkaisua.

Lokitiedot ovat Tilaajan aineistoa siltä osin kuin lokituksen kohteena on Tilaajan aineiston käsittely tai luovuttaminen. Siltä osin kuin lokitiedot ovat Tilaajan aineistoa, Toimittajan tulee toimittaa lokitiedot Tilaajan pyynnöstä ja ilman erillistä korvausta Tilaajalle tai Tilaajaan keskitettyyn lokitietojärjestelmään. Tilaaja voi myös erikseen edellyttää säännöllistä raportointia lokitiedoista.

Mikäli lokitiedot sisältävät henkilötietoja, lokitietorekisterit ovat henkilörekistereitä.

Lokitietorekisterin rekisterinpitäjä on Tilaaja, kun Toimittaja tai Ratkaisu kerää lokitietoja Tilaajan aineiston käsittelystä tai luovuttamisesta. Siltä osin kuin Tilaaja on Sopimuksessa mainittujen lokitietorekisterien rekisterinpitäjä ja Toimittaja vastaavien lokitietorekisterien henkilötietojen käsittelijä, Toimittaja vastaa lokitietorekisterissä olevien henkilötietojen käsittelyssä tässä Sopimuksessa määriteltyjen ehtojen mukaisesti. Lokitietorekistereistä täytetään osaltaan myös Sopimuksen liite 1.3 (Henkilötietojen kuvaus / seloste käsittelytoimista).

Mikäli Toimittaja toimii tässä Sopimuksessa mainittujen lokitietorekisterien rekisterinpitäjänä, Toimittaja vastaa lokitietorekisteristä Tietosuojalainsäädännön mukaisesti.

Myös lokitietorekisterin katselu ja käyttö tulee lokittaa.

Siltä osin kuin lainsäädännössä tai viranomais määräyksissä on säädetty lokitietojen keräämisestä, käsittelystä, luovuttamisesta ja säilyttämisestä, sovelletaan kyseisiä säädöksiä ja viranomais määräyksiä.

Lokitiedot ovat julkisuuslain 24 §:n mukaisesti salassapidettäviä.

7.1 Tiedonhallintalain mukaiset lokitiedot

Järjestelmän tulee kerätä tiedonhallintalain (906/2019) 17 §:ssä tarkoitetut käyttö- ja luovutuslokitiedot silloin, kun jokin seuraavista ehdoista täyttyy:

- käsitellään henkilötietoja,
- käsitellään salassa pidettäviä tietoja,
- lokitiedot ovat tarpeen käyttäjien oikeusturvan ja vastuun kannalta tai
- lokitiedot ovat tarpeen teknisten virheiden selvittämiseksi.

Käyttölokirekisteriin Toimittajan tulee kerätä tiedot Ratkaisun käytöstä, jolla tarkoitetaan tietojen tallentamista, muuttamista, poistamista, katselua tai muuta tietoihin kohdistuvaa toimenpidettä.

Luovutuslokirekisteriin Toimittajan tulee kerätä tiedot Ratkaisusta tehtävät tietojen luovutukset ja luovutusperuste. Mikäli Ratkaisusta luovutetaan tietoja tiedonhallintalain 23 §:n mukaisella katseluyhteydellä, luovutuslokirekisteriin Toimittajan tulee kerätä myös luovutusten käyttötarkoitus.

Tiedonhallintalain mukaiset lokitiedot ovat Tilaajan aineistoa ja rekisterinpitäjä on Tilaaja.

7.2 Asiakas- ja hyvinvointitietojen käsittelyn ja luovutuksen lokitiedot



Jos Pääsopimuksen kohteena on järjestelmä, johon tallennetaan asiakas- tai potilasasiakirjoja, tietojen käsittelystä on kerättävä sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (748/2021) mukainen käyttö- ja luovutusloki, johon tallennetaan tieto selatusta tai käytystä asiakas- tai potilastiedosta.

Käyttölokirekisteriin on tallennettava tieto käytetyistä asiakas- ja hyvinvointitiedoista, siitä palvelunantajasta, jonka asiakastietoja käytetään, asiakas- ja hyvinvointitietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta sekä muista käytön valvontaa ja seuranta varten tarvittavista tiedoista.

Luovutuslokirekisteriin on tallennettava tieto luovutetuista asiakastiedoista, siitä palvelunantajasta, jonka asiakastietoja luovutetaan, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta, luovutusajankohdasta sekä muista luovutusten valvontaa ja seuranta varten tarvittavista tiedoista.

Käyttö- ja luovutuslokitietojen eli lokitietoraportin avulla on pystyttävä toteamaan kyseisten käsittelytoimien perusteet, toteutuspäivä ja -aika, kenen henkilön asiakas- tai hyvinvointitietoja on käsitelty sekä henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys. Vaatimus koskee myös asiakas- ja potilastietojärjestelmän pääkäyttäjän käsittelytoimia. Lokitietoja on käytettävä ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, omaehtoiseen valvontaan, henkilötietojen eheyden ja turvallisuuden varmistamiseen, teknisten virheiden selvittämiseen sekä rikosoikeudellisiin menettelyihin.

Asiakas- ja hyvinvointitietojen käsittelyä ja luovutusta koskevat lokitiedot ovat Tilaajan aineistoa ja rekisterinpitäjä on Tilaaja.

Sosiaali- ja terveydenhuollon, pelastustoimen sekä siltä osin kuin ympäristöterveydenhuollon järjestämisvastuu siirtyy hyvinvointialueille Sopimuksessa mainittujen asiakashyvinvointitietojen sekä niihin liittyvien lokitietojen rekisterinpito siirtyy hyvinvointialueelle. Siitä lukien Toimittaja vastaa henkilötietojen käsittelystä asiakas- ja hyvinvointitietojen sekä niihin liittyvien lokitietojen osalta hyvinvointialueelle. Sopimus siirtyy Pääsopimuksen mukaisesti.

7.3 Tekniset lokit sekä tietoturvan audit trail -loki

Ratkaisun on kyettävä keräämään lokitietoa vähintään seuraavissa tapahtumissa:

- käyttäjien kirjautumiset, kirjautumisyritykset sekä uloskirjautumiset järjestelmään (**tekniinen käyttöloki**),
- Järjestelmän ylläpitotoimenpiteet (**ylläpito- ja muutosloki**) sekä
- tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tarpeelliset tekniset lokitiedot, kuten keskeisten sovellusten, käyttöjärjestelmän, verkko-laitteiden ja palvelinten lokitiedot (**tapahtuma- ja virheloki**).

Ratkaisun tapahtumista ja virheilmoituksista Toimittajan tulee kerätä lokitiedot.

Ratkaisu ei saa lokittaa pääsynhallintaan liittyviä salasanoja tai muita salassapidettäviä pääsynhallintaan liittyviä tunnuksia.

Ratkaisun tulee lokittaa kattavasti tietoa kaikista potentiaalisista tietoturvapoikkeamista. Esimerkkinä mutta ei näihin esimerkkeihin rajoittuen epäonnistuneista kirjautumisyrityksistä, salasanojen



palauttamisista, virheellisistä syötteistä sekä muista vastaavista seikoista. Lokien tulee kattaa kaikki tarvittava tieto myöhempää mahdollista tietoturvaluottokkeaman tutkintaa varten.

Teknisten ja tietoturvan audit trail -lokiens lokitiedot ovat Toimittajan aineistoa ja rekisterinpitäjänä on Toimittaja, ellei laissa ole toisin määrätty tai erikseen toisin sovittu. Toimittajan tulee edellä mainitusta huolimatta raportoida Tilaaaja tässä luvussa mainituista seikoista kuten tietoturvaluottokkeamista Pääsopimuksen mukaisesti.

7.4 Lokitietojen säilyttäminen

Lokitietoja säilytetään seuraavasti:

- luvussa 7.1 mainitut tiedonhallintalain mukaiset käyttö- ja luovutuslokit:
 - Luovutuslokit 5 v
 - Käyttölokit 2 v
- luvussa 7.2 mainitut asiakastietolain mukaiset käyttö- ja luovutuslokit 12 v
- luvussa 7.3 mainitut tekniset ja audit trail -lokit 2 v

Jos Digi- ja väestötietoviraston (DVV) väestötietoja käytetään henkilön tunnistautumisessa Suomi.fi-palvelussa tai väestötietojen muutostietopalvelua käytetään henkilön perustietojen hakemisessa, lokitietojen säilytysaika tulee olla viisi (5) vuotta.

Tilaaaja voi tapauskohtaisesti määrittellä erikseen tässä Sopimuksen kohdassa mainittuja säilytysaikojen pituuksia.

Mikäli kyseessä on lainsäädännössä säädetty lokitietojen säilyttämistä koskeva velvollisuus, lokitietoja säilytetään lainsäädännössä säädetyn ajan.

Toimittaja on vastuussa lokitietojen hävittämisestä. Toimittaja on velvollinen hävittämään lokitiedot, kun Sopimuksessa tai lainsäädännössä määritelty lokitietojen säilyttämisaika päättyy. Toimittaja toimittaa Tilaaajalle kirjallisen hävitysesityksen lokitietojen tuhoamisesta, ellei Palvelussa ole ominaisuutta, joka automaattisesti tuottaa hävitysesityksen.

Toimittajan tulee esittää Tilaaajalle kirjallinen hävitysraportti, että lokitiedot ja kaikki niistä mahdollisesti olevat jäljennökset on pysyvästi tuhottu.

Lokitietojen hävittämisen tulee sisältyä Palvelun hintaan eikä siitä saa aiheutua Tilaaajalle erillisiä kustannuksia.

7.5 Muut lokitietoja koskevat velvoitteet

Toimittajan on huolehdittava lokitietojen eheydestä ja kiistämättömyydestä siten, että ne suojataan muutoksilta. Lokitietoihin pääsy rajoitetaan vaan vain nimettyihin henkilöihin, jotka voivat hakea lokitietoja vain perustelluista syistä.

Toimittajan on Tilaaajan tai valvontaviranomaisen pyynnöstä asetettava lokitiedot Tilaaajan tai valvontaviranomaisen saataville.

Toimittajan on huolehdittava siitä, että sen käsittelemät lokitiedot ovat sähköisessä muodossa siten, että ne voidaan siirtää Palvelusta toiseen palveluun.



Lainsäädännössä määritellystä lokitietojen keräämis- ja säilyttämisvelvoitteesta osapuolet eivät voi sopia toisin.

8 Turvallisuusselvitykset

Palveluun osallistuvilta henkilöiltä Tilaaaja voi edellyttää turvallisuusselvitystä. Turvallisuusselvityksen laatii suojelupoliisi turvallisuusselvityslain ja suojelupoliisin määräysten ja ohjeiden mukaisesti, jollei toisin sovita. Jotta henkilö saa oikeuden käsitellä sellaisia salassa pidettäviä tietoja, joiden salassapito on välttämätöntä turvallisuusselvityslain (726/2014) mainittujen etujen suojaamiseksi, ja/tai päästä järjestelmiin, jotka sisältävät sellaisia salassa pidettäviä tietoja, henkilöstä tulee teettää turvallisuusselvityslain 4 luvussa tarkoitettu perusmuotoinen turvallisuusselvitys.

Tietolähteinä käytetään turvallisuusselvityslain 25 § mukaisia tietolähteitä. Mikäli turvallisuusselvitys tulee tehtäväksi ulkomailla, henkilöltä edellytetään tasoltaan vastaava ulkomainen turvallisuusselvitys. Toimittajan tulee hankkia turvallisuusselvityksen kohteena olevan henkilön suostumus selvityksen tekemiseen.

Toimittajan tulee avustaa turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta selvityksen tekemiseen. Tilaaaja vastaa turvallisuusselvityksen teettämisestä aiheutuvista viranomaiskustannuksista. Kumpikin Osapuoli vastaa muista omista kustannuksistaan erikseen.

9 Salassapito

Osapuolet huolehtivat siitä, että he toiminnassaan noudattavat EU:n ja kansallisen lainsäädännön tason säännöksiä ja määräyksiä asiakirjojen ja tietojen salassapidosta ja luottamuksellisuudesta sekä Pääsopimusta liitteineen.

Tilaaaja noudattaa julkisyhteisönä julkisuuslaissa sekä muussa lainsäädännössä olevia salassapitoa ja julkisuutta koskevia säännöksiä ja määräyksiä. Toimittaja merkitsee salassa pidettävät tiedot tai asiakirjat ”salainen”-merkinnällä tai vastaavalla salassapidettävyyttä osoittavalla merkinnällä.

Osapuolet pitävät toisiltaan saamansa salassa pidettäväksi merkityn tai muutoin salassapidettäväksi katsottavan aineiston salassa eivätkä käytä tietoja muihin kuin Pääsopimuksen mukaisiin tarkoituksiin. Osapuolet vastaavat, että kaikki heidän palveluksessaan olevat samoin kuin alihankkijat noudattavat tätä määrystä.

Osapuolella on oikeus luovuttaa toisen Osapuolen salassa pidettävää tietoa Osapuolen henkilökunnalle ja alihankkijoille sekä muille sen lukuun toimiville tahoille Pääsopimuksen mukaisia tarkoituksia varten.

Toimittaja on salassapitovelvollinen toiminnan yhteydessä tietoonsa saamiensa Tilaaajaan liittyvien tietojen, asiakirjojen ja rekistereihin sisältyvien henkilötietojen osalta.

Salassapito ja luottamuksellisuus eivät koske seuraavia tietoja:

- jotka ovat julkisessa tiedossa tai jotka olisi voitu saada laillisesti tietoon, vaikka Osapuoli ei olisi osallisena tässä Sopimuksessa;
- jotka olivat Osapuolen hallussa laillisesti jo ennen kuin toinen tämän sopimuksen Osapuoli luovutti saman tiedon;
- joiden ilmaisemiseen tai luovuttamiseen muut osapuolet ovat etukäteen antaneet kirjallisen suostumuksen; sekä



- jotka Osapuoli joutuu ilmaisemaan tai luovuttamaan häntä velvoittavan lainsäädännön tai viranomaisen antaman määräyksen tai päätöksen nojalla.

Osapuolet ymmärtävät, että vaikka jokin tieto olisi lainsäädännön perusteella julkista, niin tiedon luovuttamisesta päättää aina viranomainen. Siten Toimittajan tulee aina pyytää Tilaaajalta kirjallinen lupa tiedon luovuttamiseen Tilaaajan aineistosta sivulliselle, riippumatta siitä, onko tieto julkista tai salassapidettävää, ellei lainsäädännöstä tai viranomaismääräyksestä muuta johdu.

Osapuolet huolehtivat omilla vastuualueillaan siitä, että salassapitoa koskevia sopimusehtoja ja viranomaisten antamia määräyksiä noudatetaan myös Sopimuksen päättyessä tai purkautuessa.

Salassapidon osalta sovelletaan myös Sopimuksen liitteenä 1.1 olevaa Salassapito- ja tietoturvasitoumusta.

10 Henkilöstö

Toimittaja vastaa siitä, että Toimittajan lukuun työskentelevät henkilöt, joilla voi olla pääsy luottamuksellisiin tietoihin, ovat etukäteen allekirjoittaneet Toimittajan kirjallisen salassapitositoumuksen tai joita sitoo työ Sopimukseen perustuva salassapitovelvoite.

Toimittajan on huolehdittava siitä, että Toimittajan lukuun työskentelevät henkilöt ovat tietoisia seuraavista seikoista ja ovat sitoutuneet niitä noudattamaan:

- Työntekijä saa käyttää Tilaaajan aineistoa vain työtehtäviensä mukaiseen tarkoitukseen ja vain siinä laajuudessa kuin työtehtävien hoitaminen edellyttää. Työntekijällä ei ole oikeutta käyttää Tilaaajan aineistoa muuhun kuin edellä mainittuun tarkoitukseen.
- Työntekijän on pidettävä Tilaaajan aineisto salassa, eikä sitä saa luovuttaa tai muulla tavalla paljastaa sivullisille. Salassapitovelvollisuus on voimassa pysyvästi. Salassapitovelvollisuus ei koske julkista aineistoa.
- Sivullisina pidetään muun muassa sellaisia Toimittajan lukuun työskenteleviä henkilöitä, jotka eivät työtehtäviensä perusteella tarvitse Tilaaajan aineistoa tietoonsa.
- Työntekijän on ilmoitettava tietoonsa tulleista tietoturva- tai tietosuojaa vaarantavista seikoista Toimittajalle viipymättä.
- Työntekijän tulee käsitellä Tilaaajan aineistoa sisältäviä asiakirjoja ja tallenteita huolellisesti ja riittävästä tietoturvasta huolehtien.
- Mikäli työntekijä käyttää kannettavaa työasemaa tai mobiililaitetta, jolle on talletettu Tilaaajan aineistoa, työaseman ja mobiililaitteen suojaamisesta tulee asianmukaisesti huolehtia.
- Työntekijän pitää palauttaa hallussaan olevat asiakirjat ja tallenteet työtehtäviensä mukaisen käyttötarpeen päättyttyä.
- Tietojärjestelmien käytöstä kertyy lokitietoa, jota Sopimuksen luvun 7 mukaisesti seurataan.
- Salassapitovelvollisuuden rikkominen saattaa aiheuttaa työntekijälle lainsäädännön mukaisen henkilökohtaisen vastuun.
- Käyttäjätunnukset ja salasana ovat henkilökohtaisia, salassapidettäviä eikä niitä saa luovuttaa kenellekään muulle.
- Käyttöoikeudet tulee poistaa työntekijän käytöstä automaattisesti, kun työntekijän työtehtävät muuttuvat siten, ettei hän enää tarvitse työtehtäviensä hoitamiseen tai jos työntekijä poistuu Toimittajan palveluksesta.
- Toimittajan tulee omassa toiminnassaan varmistaa, että ylläpitotunnuksia on vain tarpeellisilla henkilöillä.
- Käyttäjätunnusten yhteiskäyttö on kielletty.



Toimittajan tulee lisäksi huolehtia siitä, että Toimittajan lukuun työskentelevät henkilöt ovat tietoisia myös muista mahdollisista Sopimuksen mukaisista salassapitovelvoitteista, ja valvoa heidän toimintansa sopimuksenmukaisuutta.

11 Tietosuoja ja tietoturvaa koskeva auditointi

Tilaaajalla on oikeus suorittaa tietosuojaan ja -turvaan liittyvän auditoinnin kerran vuodessa. Tilaaaja vastaa auditoinnin kustannuksista. Tilaaaja ja Toimittaja maksavat muut auditoinnista itselleen aiheutuneet kulunsa itse. Tilaaajan on ilmoitettava Toimittajalle kirjallisesti aikomuksestaan tehdä tai teettää Toimittajaan kohdistuva auditointi vähintään 30 päivää ennen aiotun auditoinnin ajankohtaa. Tilaaajan on myös riittävästi yksilöitävä ilmoituksessa auditoinnin kohde, paikka ja auditointi. Toimittajan tulee varata auditoinnin kohteeseen tarvittavat resurssit ja ilmoitettava ne Tilaaajalle kaksi (2) viikkoa ennen auditointia. Auditoinnin mahdollisesti aiheuttamista viivästyksistä tai muista vaikutuksista, pl. auditoinnissa havaitut Sopimuksen vastaiset virheet, ei aiheudu Toimittajalle seuraamuksia.

Auditointi voi käsittää myös Toimittajan alihankkijat siltä osin, kuin alihankkijat osallistuvat tämän sopimuksen mukaisten velvollisuuksien täyttämiseen. Auditoinnin käsitteessä Toimittajan alihankkijat, sovitaan menettelystä, kustannusten jaosta ja muista seikoista tietosuojayhteistyöselimessä.

Tilaaaja voi käyttää kolmatta osapuolta apuna auditoinnissa. Toimittajan suora kilpailija ei voi toimia auditointina. Auditointia sitoo turvallisuutta ja salassapitoa koskevat ehdot ja Tilaaaja vastaa siitä, että auditointi noudattaa näitä ehtoja.

Tilaaaja voi myös hyödyntää Toimittajan suostumuksella kolmannen, Tilaaajan hyväksymän auditoinnin, tuloksia, mikäli kolmas osapuoli on auditoinut Tilaaajan haluaman auditointia Toimittajan palvelun viimeisen kahdentoista (12) kuukauden aikana Tilaaajan auditointia koskevasta ilmoituksesta. Mikäli Tilaaaja hyväksyy jo tehdyn auditoinnin tulokset, uutta auditointia ei tarvitse tehdä hyväksytyiltä osin. Tässä kohdassa mainituista auditoinnista aiheutuvista kuluista ei vastaa Tilaaaja.

Auditoinnin tulokset käsitellään Sopijapuolten kesken. Toimittajalla on velvollisuus korjata auditoinnissa havaitut Sopimuksen vastaiset virheet ilman Tilaaajalta perittäviä lisäkustannuksia viipymättä, kuitenkin viimeistään 14 vuorokauden sisällä, ellei muuta kirjallisesti erikseen sovita.

Toimittaja on velvollinen tarjoamaan auditointia varten tarvittaviin tiloihin ja järjestelmiin sekä tarvittavan avun auditoinnin suorittamiseksi. Auditointi ei saa vaarantaa Toimittajan muiden asiakkaiden tietoturvaa tai salassapitovelvoitteita, eikä se saa muutoin haitata merkittävästi Toimittajan muuta liiketoimintaa. Mikäli Toimittajan tietoturva- ja salassapitovelvoitteet estävät auditointia varten tarvittaviin tiloihin tai järjestelmiin, Toimittaja varmistaa, että auditointi saa oleelliset tiedot auditointia varten.

12 Korvausvastuu ja vastuunrajoitukset

Korvausvastuuseen ja vastuunrajoituksiin sovelletaan Pääsopimusta.

13 Muut ehdot

Muiden ehtojen osalta noudatetaan sitä, mitä Pääsopimuksessa on sovittu.



14 Voimaan jäävät ehdot

Sopimuksen ehdot ovat voimassa viisi (5) vuotta Pääsopimuksen päättymisen jälkeen, ellei lainsäädännöstä muuta johdu.

15 Sopimuksen voimaantulo

Sopimus tulee voimaan, kun molemmat Sopijapuolet ovat sen allekirjoittaneet.

16 Sopimuksen voimassaolo

Sopimuksen voimassaolo on Pääsopimuksen mukainen.

17 Sopimusasiakirjat ja soveltamisjärjestys

Sopimukseen sisältyvät asiakirjat ovat:

Pääsopimuksen liite 1 Tietoturvaluussopimus

Pääsopimuksen liite 1.1 Salassapito- ja tietoturvasitoumus

Pääsopimuksen liite 1.2 Henkilötietojen käsittelyn vaatimukset

Pääsopimuksen liite 1.3 Henkilötietojen kuvaus / seloste käsittelytoimista

Pääsopimuksen liite 1.4 Henkilötietojen tietoturvaloukkausten selvittäminen

Pääsopimuksen liite 1.5 Yhteyshenkilöt

Sopimukseen sovelletaan Pääsopimuksen soveltamisjärjestystä.

18 Sopimuskappaleet ja allekirjoitukset

Sopimusta on laadittu kaksi (2) samasanaista kappaletta, yksi (1) kummallekin Sopijapuolelle, Sopijapuolten asianmukaisesti valtuuttamien allekirjoittajien toimesta.

Allekirjoitettu sähköisesti Pääsopimuksen yhteydessä.