**Vantaan ja Keravan hyvinvointialue**

**Tietoturvallisuussopimus**

SISÄLLYSLUETTELO

1 Sopimuksen osapuolet 3

2 Määritelmät 3

3 Sopimuksen tausta 4

4 Sopimuksen kohde 4

5 Tietoturva 4

6 Tietosuoja 5

7 Lokitiedot 7

7.1 Tiedonhallintalain mukaiset lokitiedot 8

7.2 Asiakas- ja hyvinvointitietojen käsittelyn ja luovutuksen lokitiedot 8

7.3 Tekniset lokit sekä tietoturvan audit trail -loki 9

7.4 Lokitietojen säilyttäminen 9

7.5 Muut lokitietoja koskevat velvoitteet 10

8 Salassapito 10

9 Henkilöstö 11

10 Tietosuojaa ja tietoturvaa koskeva auditointi 12

11 Muut ehdot 13

12 Voimaan jäävät ehdot 13

13 Sopimuksen voimaantulo 13

14 Sopimuksen voimassaolo 13

15 Sopimuksen liitteet ja soveltamisjärjestys 13

16 Sopimuskappaleet ja allekirjoitukset 14

Tietoturvallisuussopimus

# Sopimuksen osapuolet

**Palvelun järjestäjä:** Vantaan ja Keravan hyvinvointialue (Myöhemmin ”VAKE” tai ”Sopijapuoli”)

Y-tunnus: 3221356-1

Osoite: PL 1700

01030 VANTAAN KAUPUNKI

**Toimittaja:** Nimi:

Osoite:

Puh:

Internet-sivut:

Y-tunnus:

(Myöhemmin ”Toimittaja” tai ”Sopijapuoli”)

Yhdessä myös ”Sopijapuolet”.

# 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** Palvelusetelisääntökirjan kohteena olevat palvelut.

**Sopimus:Tämä sopimus.**

**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 sääntökirjan määritelmiä.

# Sopimuksen kohde

Sopimuksen kohteena on VAKEn palvelusetelillä järjestämän palvelun tietosuoja- ja tietoturvaehdot. Toimittajan tulee noudattaa ehtoja tuottaessaan VAKEn asiakkaalle sääntökirjan mukaisia palveluja.

Toimittaja täyttääliitteen 1.3 (liite 1.3 Henkilötietojen kuvaus / seloste käsittelytoimista).

VAKE voi päätöksellään keskeyttää tai lopettaa Toimittajan Palvelujen käytön kokonaan tai osittain väliaikaisesti, jos sen toiminnassa ilmenee vakavia tietosuoja- tai tietoturvapuutteita. VAKE jatkaa Palvelujen käyttöä, kun tietosuoja- tai tietoturvapuutteet Toimittajan toiminnassa on korjattu. Osapuolet ymmärtävät, ettei Toimittajalla ole oikeutta veloittaa Palvelujen käytöstä siltä osin, kuin VAKE on päätöksellään keskeyttänyt tai lopettanut Palvelujen käytön.

Sopijapuolten 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.

# Tietoturva

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

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

Toimittajan velvollisuutena on huolehtia vaatimuksenmukaisesta 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, sopimuksessa tai sääntökirjassa toisin edellytetä. Toimittaja on velvollinen puolivuosittain, ellei toisin erikseen sovita, todentamaan kirjallisesti VAKElle, että varmistuskopiointi on onnistunut ja tietojen eheys on säilynyt sekä myös tietojen palautus onnistuu.

Toimittaja vastaa VAKEn 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 VAKE tai VAKEn vastuulla oleva aiheuttaa omalla toiminnallaan tietojen tai tiedostojen katoamisen taikka häviämisen taikka mikäli tietojen tai tiedostojen katoaminen aiheutuu Toimittajan vaikutusvallan ulkopuolella olevasta seikasta. Selvyyden vuoksi todetaan kuitenkin, että Toimittaja on kuitenkin viimeksi mainitussa tapauksessa velvollinen erillistä korvausta vastaan palauttamaan VAKEn tiedot ja auttamaan VAKEa tietojen ajantasaistamisessa.

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

* Toimittajan tietoturva- ja tietosuojapolitiikka,
* Toimittajan asiakkaiden käyttäjätunnusten hallinnan periaatteet,
* Toimittajan lokienhallinnan periaatteet,
* Toimittajan varmistusten hallinnan periaatteet,
* Toimittajan toipumissuunnitelma sekä
* Toimittajan tietoturvapäivitysten hallinta.

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

Lisäksi Toimittajan on toimitettava suunnitelma ja menettelytavat tietoturvaloukkausten varalle.

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

# Tietosuoja

Toimittajan tulee kaikessa sääntökirjan mukaisten velvoitteidensa täyttämisessä noudattaa voimassa olevaa tietosuojaa koskevaa Euroopan unionin ja kansallista lainsäädäntöä.

Toimittaja vastaa siitä, että sääntökirjan 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 VAKEn aineiston luottamuksellisuuden, eheyden ja saatavuuden.

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

Toimittajalla on oikeus käsitellä VAKEn aineistoon sisältyviä Henkilötietoja:

* vain sääntökirjassa mainitulla perusteella tai VAKEn kirjallisesti etukäteen antamalla luvalla,
* vain siinä määrin ja niin kauan, kuin se on sääntökirjan kohteen toteuttamiseksi välttämätöntä sekä
* vain tämän Sopimuksen ja sääntökirjan sekä VAKEn erikseen antamien dokumentoitujen ohjeiden mukaisesti.

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

Henkilötietojen käsittelyn käsittelyperuste on yksilöity Sopimuksen liitteessä 1.3.

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

Toimittajan tulee ilmoittaa EU:n yleisen tietosuoja-asetuksessa määritellyistä henkilötietojen tietoturvaloukkauksista VAKElle välittömästi, kuitenkin viimeistään 36 tunnin kuluessa siitä, kun Toimittaja tai sen mahdollinen alihankkija on havainnut tietoturvaloukkauksen. Toimittajan on ilman aiheetonta viivytystä toimitettava kirjallinen selvitys tapahtumasta sekä lisäselvityksiä sitä mukaa kuin Toimittaja saa tapahtumasta lisätietoa. 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 VAKElle, rekisteröidylle tai kolmannelle osapuolelle, Toimittaja vastaa vahinkojen korvaamisesta lainsäädännön mukaisesti.

Toimittajan on korvattava VAKElle sopimusrikkomuksesta aiheutunut vahinko täysimääräisesti mukaan lukien VAKElle rikkomuksen perusteella mahdollisesti määrätyt GDPR:n mukaiset hallinnolliset sanktiot ja kolmannelle maksettavat korvaukset.

Toimittaja on velvollinen puolustamaan kustannuksellaan VAKEa, jos rekisteröity väittää, että VAKE on loukannut rekisteröidyn yksityisyyden suojaa ja väitetty loukkaus johtuu Toimittajasta.

Mikäli VAKE joutuu oikeudellisesti puolustautumaan tietoturva- tai tietosuojaloukkausta vastaan, Toimittajan on toimitettava ilman aiheetonta viivytystä VAKEn käyttöön kaikki hallussaan oleva asiaan liittyvä aineisto sekä avustamaan VAKEa puolustautumistoimenpiteissä. Aineisto on toimitettava ilman erillistä korvausta. 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. Toimittajan lopetettua sääntökirjan mukaisen palvelun tuottamisen VAKElle tai Henkilötietojen käsittelytarkoituksen päätyttyä Toimittajalle ei jää VAKEn henkilöstön tai asiakkaiden henkilötietoja, ellei lainsäädännöstä muuta johdu.

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

# Lokitiedot

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

Mikäli lokitiedot sisältävät henkilötietoja, lokitietorekisterit ovat henkilörekistereitä.

Lokitietorekisterin rekisterinpitäjä on VAKE, kun Toimittaja tai Ratkaisu kerää lokitietoja VAKEn aineiston käsittelystä tai luovuttamisesta. Siltä osin kuin VAKE 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 viranomaismääräyksissä on säädetty lokitietojen keräämisestä, käsittelystä, luovuttamisesta ja säilyttämisestä, sovelletaan kyseisiä säädöksiä ja viranomaismääräyksiä.

[Tarvittavat lokitiedot on voitava siirtää VAKEn niin päättäessä VAKEn keskitettyyn lokitietojärjestelmään.]

## 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 VAKEn aineistoa ja rekisterinpitäjä on VAKE.

[Tarvittavat lokitiedot on voitava siirtää VAKEn niin päättäessä VAKEn keskitettyyn lokitietojärjestelmään.]

## Asiakas- ja hyvinvointitietojen käsittelyn ja luovutuksen lokitiedot

Jos sääntökirjan 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 käytetystä 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 seurantaa 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 seurantaa 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 VAKEn aineistoa ja rekisterinpitäjä on VAKE.

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

[Tarvittavat lokitiedot on voitava siirtää VAKEn niin päättäessä VAKEn keskitettyyn lokitietojärjestelmään.]

## Tekniset lokit sekä tietoturvan audit trail -loki

Ratkaisun on kyettävä keräämään lokitietoa vähintään seuraavissa tapahtumissa:

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

Ratkaisun tapahtumista ja virheilmoituksista Toimittajan tulee kerätä lokitiedot.

Ratkaisu ei saa lokittaa pääsynhallintaan liittyviä salaisuuksia, kuten salasanoja tai pääsytunnuksia.

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 tietoturvapoikkeaman tutkintaa varten.

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

## 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

VAKE voi tapauskohtaisesti määritellä 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 VAKElle kirjallisen hävitysesityksen lokitietojen tuhoamisesta, ellei Palvelussa ole ominaisuutta, joka automaattisesti tuottaa hävitysesityksen.

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

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

## 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 VAKEn tai valvontaviranomaisen pyynnöstä asetettava lokitiedot VAKEn 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.

# Salassapito

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

VAKE 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 salassapidettäviksi katsottavan aineiston salassa eivätkä käytä tietoja muihin kuin sääntökirjan mukaisiin tarkoituksiin. Osapuolet vastaavat, että kaikki heidän palveluksessaan olevat samoin kuin alihankkijat noudattavat tätä määräystä.

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

Toimittaja on salassapitovelvollinen toiminnan yhteydessä tietoonsa saamiensa VAKEen 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 VAKElta kirjallinen lupa tiedon luovuttamiseen sivulliselle, riippumatta siitä, onko tieto julkista tai salassapidettävää.

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.

Lokitiedot ovat julkisuuslain 24 §:n mukaisesti salassapidettäviä.

# Henkilöstö

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

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

* Työntekijä saa käyttää VAKEn aineistoa vain työtehtäviensä mukaiseen tarkoitukseen ja vain siinä laajuudessa kuin työtehtävien hoitaminen edellyttää. Työntekijällä ei ole oikeutta käyttää VAKEn aineistoa muuhun kuin edellä mainittuun tarkoitukseen.
* Työntekijän on pidettävä VAKEn 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 VAKEn aineistoa tietoonsa.
* Työntekijän on ilmoitettava tietoonsa tulleista tietoturvaa tai tietosuojaa vaarantavista seikoista Toimittajalle viipymättä.
* Työntekijän tulee käsitellä VAKEn aineistoa sisältäviä asiakirjoja ja tallenteita huolellisesti ja riittävästä tietoturvasta huolehtien.
* Mikäli työntekijä käyttää kannettavaa työasemaa tai mobiililaitetta, jolle on talletettu VAKEn aineistoa, työaseman ja mobiililaitteen suojaamisesta tulee asianmukaisesti huolehtia.
* Työntekijän pitää palauttaa hallussaan olevat asiakirjat ja tallenteet työtehtäviensä mukaisen käyttötarpeen päätyttyä.
* Tietojärjestelmien käytöstä kertyy lokitietoa, jota Sopimuksen liitteen 1.2 kohdan 6 mukaisesti seurataan.
* Salassapitovelvollisuuden rikkominen saattaa aiheuttaa työntekijälle lainsäädännön mukaisen henkilökohtaisen vastuun.
* Käyttäjätunnukset ja salasanat ovat henkilökohtaisia, salassapidettäviä eikä niitä saa luovuttaa kenellekään muulle.

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

# Tietosuojaa ja tietoturvaa koskeva auditointi

VAKElla on oikeus suorittaa tietosuojaan ja -turvaan liittyvän auditoinnin kerran vuodessa. VAKE vastaa auditoijan kustannuksista. VAKE ja Toimittaja maksavat muut auditoinnista itselleen aiheutuneet kulunsa itse. VAKEn on ilmoitettava Toimittajalle kirjallisesti aikomuksestaan tehdä tai teettää Toimittajaan kohdistuva auditointi vähintään 30 päivää ennen aiotun auditoinnin ajankohtaa. VAKEn on myös riittävästi yksilöitävä ilmoituksessa auditoinnin kohde, paikka ja auditoija. Toimittajan tulee varata auditoinnin kohteeseen tarvittavat resurssit ja ilmoitettava ne VAKElle 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 käsittäessä Toimittajan alihankkijat, sovitaan menettelystä, kustannusten jaosta ja muista seikoista tietosuojayhteistyöelimessä.

VAKE voi käyttää kolmatta osapuolta apuna auditoinnissa. Toimittajan suora kilpailija ei voi toimia auditoijana. Auditoijaa sitoo turvallisuutta ja salassapitoa koskevat ehdot ja VAKE vastaa siitä, että auditoija noudattaa näitä ehtoja.

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

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

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

# Muut ehdot

Muiden ehtojen osalta noudatetaan sitä, mitä sääntökirjassa on edellytetty.

Sopijapuolet sitoutuvat pitämään tämän Sopimuksen sisällön liitteineen salaisena, ellei viranomaistoimintaa koskevasta lainsäädännöstä muuta johdu.

# Sopimuksen voimaantulo

Sopimus tulee voimaan, kun toimittaja on hyväksynyt sääntökirjan ja sopimuksen VAKEn määrittämällä tavalla.

# Sopimuksen voimassaolo

Tämän sopimuksen mukainen salassapitovelvollisuus on voimassa myös sen jälkeen, kun Palveluntuottajan velvollisuus Palvelun tuottamiseen on päättynyt.

Velvoitteet, joiden on niiden luonteen vuoksi tarkoitus säilyä voimassa tämän sopimuksen voimassaolon päättymisestä riippumatta, jäävät voimaan sopimuksen päättymisen jälkeen.

# Sopimuksen liitteet ja soveltamisjärjestys

Sopimuksen liitteet ovat

1.1 Salassapito- ja tietoturvasitoumus

1.2 Henkilötietojen käsittelyn vaatimukset

1.3 Henkilötietojen kuvaus / seloste käsittelytoimista

1.4 Henkilötietojen tietoturvaloukkausten selvittäminen