25.9.2018

TIETOTURVALLISUUSLIITE

HELSINGIN KAUPUNKI

Sisällys

25.9.2018

A. JOHDANTO

1. Määritelmät

(1) **Alihankkija** tarkoittaa Pääsopimuksen mukaisia alihankkijoita.

(2) **Palvelu** tarkoittaa sitä palvelua, josta Tilaaja ja Toimittaja ovat sopineet Pääsopimuksessa. Tässä Tietoturvallisuusliitteessä Palvelulle asetettuja velvoitteita sovelletaan soveltuvin osin myös Pääsopimuksessa mahdollisesti sovittuun projektiin sekä järjestelmä- ja tavarahankintaan.

(3) **Pääsopimus** tarkoittaa Tilaajan ja Toimittajan välillä tehtyä sopimusta.

(4) **Salassa pidettävä tieto** tarkoittaa kaikkea sellaista tietoa tiedon muodosta riippumatta, jonka Sopijapuoli on luovuttanut toiselle Sopijapuolelle, tai jonka Tilaaja on tallentanut Palveluun, tai joka on syntynyt Palvelun tuottamisessa, tai jonka Sopijapuoli 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 Sopijapuoli on merkinnyt salassa pidettäväksi tai jonka toinen Sopijapuoli tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin; tai
iv. kyse on henkilötiedoista tai henkilörekisteristä.

(5) **Sopijapuolet** tarkoittaa Pääsopimuksessa määriteltyjä **Tilaajaa** ja **Toimittajaa**.

(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) **Tietoturvallisuusliite** tarkoittaa tätä Pääsopimuksen liitteenä olevaa asiakirjaa.

2. Yhteyshenkilöt

(1) Tilaajan yhteyshenkilö tietoturvallisuusasioissa:

Nimi: Mikko Paananen
Titteli: SAP manager
Sähköposti: mikko.paananen@hel.fi
Puhelinnumero: 0407721728

(2) Toimittajan yhteyshenkilö tietoturvallisuusasioissa:

Nimi: Eija Rantanen
Titteli: johtaja
Sähköposti: eija.rantanen@cgi.com
Puhelinnumero: +358 40 578 6070

(3) Sopijapuolet sitoutuvat ilmoittamaan välittömästi toisilleen tietoturvallisuudesta vastaavan yhteyshenkilön vaihtumisesta.

3. Tietoturvallisuusliitteen tausta ja tarkoitus

(1) Sopijapuolet ovat tehneet Pääsopimuksen, jolla Sopijapuolet ovat sopineet Palvelun tuottamisesta.

(2) Mikäli Palveluun sisältyy henkilötietojen käsittelyä, Sopijapuolet ovat sopineet Pääsopimuksessa 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)

(3) Tässä Tietoturvallisuusliitteessä määritellään Sopijapuolten välillä noudatettavat turvallisuusjärjestelyt ja Salassa pidettävää tietoa koskevat järjestelyt Pääsopimuksen sisältämän Palvelun tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Sopijapuolten välisessä yhteistyössä.

(4) Sopijapuolet tiedostavat, että Pääsopimuksen perusteella toimitettavaan Palveluun sisältyy sellaista tietoa, jonka salassa pysyminen voi olla mm. Tilaajan ja yksilöiden turvallisuuden ja oikeuksien, Tilaajan toiminnan, lainsäädännön asettamien oikeuksien ja velvollisuuksien sekä viranomaisia ja yksilöitä sitovien ohjeiden noudattamisen kannalta kriittistä. Tällä Tietoturvallisuusliitteellä Sopijapuolet pyrkivät varmistamaan, että Salassa pidettävät tiedot pysyvät salassa ja Palvelun tuottamisessa noudatetaan tietoturvallisuutta koskevaa lainsäädäntöä.

(5) Huolimatta siitä, mitä muissa Sopijapuolten välisissä sopimusasiakirjoissa on mahdollisesti sovittu tämän Tietoturvallisuusliitteen piiriin kuuluvista asioista tai niihin liittyvistä vastuista taikka sopimusasiakirjojen keskinäisestä pätevyysjärjestyksestä, tätä Tietoturvallisuusliitettä sovelletaan aina ensisijaisesti tämän Tietoturvallisuusliitteen piiriin kuuluvissa asioissa.

(6) Mikäli Pääsopimukseen sovelletaan JIT 2015 Yleisiä ehtoja, tätä Tietoturvallisuusliitettä sovelletaan kyseisten ehtojen kohdan 18 sijaan. Mikäli Pääsopimukseen sovelletaan JIT 2015 Palvelut verkon kautta -ehtoja, tätä Tietoturvallisuusliitettä sovelletaan kyseisten ehtojen kohtien 13 ja 14 sijaan.

4. Alihankinta

(1) Toimittaja ei saa ilman Tilaajan antamaa kirjallista ennakkolupaa käyttää henkilötietojen käsittelyyn muita alihankkijoita kuin Pääsopimuksessa määritellyt Alihankkijat. Toimittajan on tiedotettava Tilaajalle kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat henkilötietojen käsittelijöinä toimivien alihankkijoiden lisäämistä tai vaihtamista, ja annettava Tilaajalle mahdollisuus vastustaa tällaisia muutoksia.

(2) Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tämän Tietoturvallisuusliitteen ehtoja myös käyttäessään Alihankkijoita. Toimittajan on tiedotettava Alihankkijalle tämän Tietoturvallisuusliitteen mukaisista velvoitteista sekä siitä, että toiminnan saattamisesta Tietoturvallisuusliitteen edellyttämälle tasolle saattaa aiheutua kustannuksia. Tilaaja ei vastaa näistä kustannuksista.

(3) Toimittaja vastaa siitä, että sen Alihankkijat toimivat tämän Tietoturvallisuusliitteen ehtojen mukaisesti. Toimittaja vastaa Alihankkijoistaan samalla tavoin kuin omasta toiminnastaan.

(4) Toimittaja vastaa siitä, että Alihankkijan työntekijät, jotka osallistuvat Palvelujen toimittamiseen Tilaajalle, ovat tietoisia ja sitoutuneita noudattamaan tämän Tietoturvallisuusliitteen ehtoja.

(5) Tässä Tietoturvallisuusliitteessä Toimittajan henkilöstölle asetettavia velvoitteita sovelletaan myös Alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.

B. TIETOTURVALLISUUS JA SALASSAPITO

5. Sopijapuolten yleiset velvoitteet

(1) Toimittaja ja sen alihankkija noudattavat tätä Tietoturvallisuusliitettä ja Tilaajan tietoturvallisuusohjeita Palvelun tuottamisessa. Lisäksi Toimittaja ja sen alihankkija noudattavat Toimittajan sisäisiä tietoturvallisuusohjeita siltä osin, kuin ne eivät ole ristiriidassa Pääsopimuksen, Pääsopimuksen liitteiden, tämän Tietoturvallisuusliitteen tai Tilaajan tietoturvallisuusohjeiden kanssa.

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

(3) Toimittaja vastaa siitä, ettei Tilaajan tietojen tai Salassa pidettävien tietojen luottamuksellisuus, saatavuus tai eheys vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Tietoturvallisuusliitteen tai Pääsopimuksen vastaisen toiminnan johdosta.

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

(5) Tilaaja vastaa siitä, että se noudattaa omassa toiminnassaan tätä Tietoturvallisuusliitettä ja tietosuojaa koskevaa lainsäädäntöä ja pyrkii kaikin kohtuullisin keinoin myötävaikuttamaan Toimittajan mahdollisuuksiin toimia tämän liitteen mukaisesti.

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

6. Toimittajan tietoturvallisuus

(1) Toimittaja informoi Tilaajaa Palvelun tietoturvallisuudesta ja muista vaatimustenmukaisuuteen liittyvistä seikoista pitämällä Tilaajaan aktiivisesti yhteyttä ja siten, että Tilaaja on niistä jatkuvasti tietoinen.

(2) Toimittaja sitoutuu toteuttamaan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet Salassa pidettävien tietojen käsittelyn turvallisuuden varmistamiseksi ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit sekä noudattamaan Tilaajan ohjeita ja mahdollisia Tilaajan ohjeiden päivityksiä.

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

(4) Toimittaja vastaa siitä, että sen ja sen Alihankkijan henkilöstön käytettävissä on helposti saatavilla olevat ajantasaiset ja asianmukaiset tämän Tietoturvaliitteen mukaiset tietosuojaan liittyvät ohjeistukset ja dokumentit.

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

6.1 Henkilöstöturvallisuus ja turvallisuusselvitykset

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

(2) Tilaaja voi edellyttää turvallisuusselvityksistä annetussa laissa (726/2014) tarkoitettua turvallisuusselvitystä tai tarvittaessa tasoltaan vastaavaa ulkomaista turvallisuusselvitystä Palvelun tuottamiseen osallistuvista Toimittajan tai sen Alihankkijan työntekijöistä, jotka käsittelevät Salassa pidettäviä tietoja tai pääsevät järjestelmiin, jotka sisältävät Salassa pidettäviä tietoja.

(3) Turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta vastaa Toimittaja. Toimittajan tulee toimittaa turvallisuusselvityksen kohteena olevan henkilön täyttämä ja allekirjoittama turvallisuusselvityshakemuslomake Tilaajalle turvallisuusselvityksen teettämistä varten.

(4) Tilaaja vastaa edellä kuvattujen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai sen Alihankkijan henkilöstössä tapahtuu Tilaajasta riippumaton vaihdos tai lisäys, Toimittaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.

6.2 Tietoaineistoturvallisuus

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

(2) Tilaaja luokittelee Tietoaineistot luottamuksellisuuden perusteella ja tietojärjestelmät kriittisyyden perusteella. Luokitusten muutoksista sovitaan erikseen kirjallisesti.

(3) Tilaaja määrittelee kullekin luokalle tietoturvallisuustason ja sen mukaiset tietoturvatoimenpiteet ja -ohjeet.

(4) Toimittaja käsittelee Tilaajan tietoaineistoja niiden turvallisuusluokkien edellyttämällä tavalla.

6.3 Pääsy tiloihin

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

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

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

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

6.4 Pääsy järjestelmiin ja tietoihin

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

(2) Toimittaja vastaa siitä, että kohdassa 6.4(1) tarkoitetut henkilöt noudattavat tätä Tietoturvallisuusliitettä.

(3) Toimittaja vastaa siitä, että kohdassa 6.4(1) tarkoitettu henkilö on tehnyt kirjallisen, tämän Tietoturvaliitteen mukaisen salassapitositoumuksen ennen kuin hän aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin. Tilaajan pyynnöstä kyseinen salassapitositoumus on esitettävä Tilaajalle.

(4) Toimittajan käyttöoikeudet Tilaajan järjestelmiin tarkastetaan säännöllisesti vähintään vuoden välein ja tarpeettomat tai liian laajat käyttöoikeudet poistetaan. Pääsääntöisesti käytetään vain käyttäjäkohtaisia tunnuksia. Yhteiskäyttöiset käyttäjätunnukset ovat sallittuja vain Tilaajan luvalla.

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

7. Tietoturvaloukkausten käsittely

(1) Palveluun liittyvistä tietoturvapoikkeamista Toimittaja on velvollinen kirjallisesti ilmoittamaan Tilaajalle välittömästi saatuaan sen tietoonsa ja viimeistään 36 tunnin kuluessa tiedoksisaannista. Ilmoitusvelvollisuus koskee ainakin toteutuneita tietovuotoja/-murtoja, tietomurron yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia sekä muita vastaavaa poikkeamia, jotka ovat omiaan nostamaan riskiä Tilaajan Salassa pidettävien tietojen luottamuksellisuuden vaarantumiselle.

(2) Lisäksi Toimittaja sitoutuu ilmoittamaan Tilaajalle muista Toimittajan tuottaman palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia Tilaajan Salassa pidettävien tietojen luottamukselliselle käsittelylle tai sellaisten henkilöiden asemaan ja oikeuksiin, joiden henkilötietoja Toimittaja käsittelee. Ilmoitus on tehtävä edellä mainitussa määräajassa, ellei Sopimuksessa tai sen liitteissä ole sovittu lyhyemmästä määräajasta.

(3) Toimittajan on annettava Tilaajalle 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 Toimittaja ehdottaisi tai joita se on toteuttanut tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

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

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

(6) Toimittaja on velvollinen auttamaan Tilaajaa tietoturvapoikkeamiin liittyvien vahinkojen minimoinnissa.

(7) Rikos- ja väärinkäyttötapauksissa tai sellaisia epäiltäessä Tilaaja ja Toimittaja pyrkivät olosuhteet ja lainsäädännön vaatimukset huomioon ottaen neuvottelemaan jatkotoimenpiteistä. Toimittajalla on velvollisuus avustaa Tilaajaa asian selvittämisessä viranomaistahojen kanssa.

8. Tietoturvallisuuteen liittyvä muutoshallinta ja kehittäminen

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

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

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

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

(5) Tämän Tietoturvallisuusliitteen yhteyshenkilöt vastaavat tämän liitteen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan yhteyshenkilöiden kesken vähintään kahden vuoden välein.

(6) Tähän Tietoturvallisuusliitteeseen tehtävät muutokset tulee tehdä kirjallisesti ja molempien Sopijapuolten tulee vahvistaa ne allekirjoituksellaan. Tämän Tietoturvallisuusliitteen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

9. Salassapito

(1) Sopijapuolet soveltavat tässä Tietoturvallisuusliitteessä määriteltyjä turvallisuusjärjestelyitä aina Toimittajan tai sen Alihankkijan käsitellessä Salassa pidettävää tietoa.

(2) Tilaaja noudattaa julkisyhteisönä julkisuuslaissa sekä muussa lainsäädännössä olevia salassapitoa, julkisuutta ja yksityisyydensuojaa koskevia säännöksiä. Tällä Tietoturvaliitteellä ei voida poiketa lainsäädännön Tilaajalle asettamista pakottavista velvoitteista.

(3) Toimittajan 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)
- Henkilötietolaki (523/1999)
- EU:n tietosuoja-asetus (EU 2016/679)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Tietoyhteiskuntakaari (917/2014)
- Laki yksityisyyden suojasta työelämässä (759/2004)

(4) Sopijapuolet pitävät salassa kaikki Salassa pidettävät aineistot ja tiedot. Salassa pidettäviä tietoja ei saa käyttää omaksi tai toisen hyödyksi tai vahingoksi.

(5) Sopijapuolet säilyttävät ja käsittelevät Salassa pidettävää tietoa siten, että se pysyy vain niiden henkilöiden hallussa, joilla on oikeus Salassa pidettävään tietoon, eikä se joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

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

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

(8) Tilaaja päättää tiedon antamisesta asiakirjasta, joka on saatu Tilaajalta tai joka on laadittu Tilaajan toimeksiantotehtävää suoritettaessa.

(9) Pääsopimuksen päättyessä Toimittaja ja sen Alihankkijat palauttavat Tilaajan Salassa pidettävää tietoa sisältävän aineiston ja muun Tilaajan osoittaman Tilaajalle kuuluvan aineiston sekä hävittävät taltioillaan olevan tietoaineiston ja kopiot. Aineistoa ei saa hävittää, mikäli Tilaaja, laki tai viranomaisten määräykset

vaativat sen säilyttämistä. Tällöin Tilaaja ohjeistaa Toimittajaa tarkemmin siitä, miten sen tulee menetellä.

(10) Salassapitovelvollisuus on voimassa myös sen jälkeen, kun Tilaajan ja Toimittajan välinen Pääsopimus on päättynyt.

C. HENKILÖTIETOJEN KÄSITTELY

10. Henkilötietojen käsittely

(1) Tilaaja on Tietosuoja-asetuksen ja henkilötietolain (523/1999) mukaisten henkilötietojen rekisterinpitäjä ja vastaa näiden tietojen käsittelystä. Toimittaja huolehtii omalta osaltaan siitä, että Toimittaja ja sen alihankkijat noudattavat rekisterinpitäjän lukuun toimivalle henkilötietolain 5 §:ssä asetettua huolellisuusvelvoitetta. Osapuolet ymmärtävät, että rekisterinpitäjänä Tilaaja saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää voimassaolevan henkilötietojen käsittelyyn ja tietosuojaan liittyvän lainsäädännön vaatimukset ja 25.5.2018 alkaen EU:n yleisen tietosuoja-asetuksen vaatimukset, ja että sillä varmistetaan rekisteröidyn oikeuksien suojelu.

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

(3) Toimittaja käsittelee henkilötietoja Tilaajan toimeksiannosta vain siinä määrin kuin se on Palvelun tuottamiseksi tarpeen ja vain siihen saakka, kunnes Pääsopimuksen voimassaoloaika on päättynyt tai Toimittajan avustamisvelvollisuus on päättynyt Tilaajan ohjeistuksen mukaisesti. Toimittajalla ei ole oikeutta käyttää saamiaan henkilötietoja omassa toiminnassaan, käsitellä niitä tämän Tietoturvallisuusliitteen vastaisesti, yhdistää henkilötietoja muuhun hallussaan olevaan aineistoon eikä luovuttaa niitä. Tilaaja ohjeistaa Toimittajaa henkilötietojen siirtoon tai tuhoamiseen liittyvästä menettelystä Pääsopimuksen päättämisen yhteydessä.

(4) Toimittaja ei saa siirtää tai luovuttaa Tilaajan henkilötietoja EU tai ETA-alueen ulkopuolelle. Palvelimien tulee sijaita EU- tai ETA-alueella ja Toimittajan tulee ilmoittaa Tilaajalle niiden sijoituspaikat. Toimittajan on ilmoitettava Tilaajalle etukäteen, jos palvelimien sijaintipaikka muuttuu. Jos Pääsopimuksessa on sovittu käsittelyn ja palvelinten sijainnista tästä poikkeavasti, sovelletaan Pääsopimusta.

(5) Mikäli rekisteröidyllä on oikeus saada tiedot koneellisessa muodossa, Toimittajan on huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan automaattisesti irrottaa järjestelmästä siirrettäväksi toiseen järjestelmään.

(6) Toimittaja on velvollinen tallentamaan lokitiedot kaikista henkilötietojen käsittelytoimista, mukaan lukien henkilötietojen katselusta. Tilaajan pyynnöstä Toimittaja antaa kyseiset lokitiedot Tilaajalle. Lokitietoihin liittyvistä velvoitteista sovitaan tarkemmin Pääsopimuksessa tai sen liitteissä.

(7) Toimittajan ja sen Alihankkijan on pyynnöstä tehtävä Tietosuoja-asetuksen 31 artiklan mukaisesti yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

(8) Toimittajan on tarvittaessa avustettava Tilaajaa Tietosuoja-asetuksen 35 artiklan mukaisen vaikutusten arvioinnin tekemisessä ja 36 artiklan mukaisen ennakkokuulemisen toteuttamisessa.

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

(10) Toimittajan on nimettävä Tietosuoja-asetuksen 37 artiklan mukaisesti tietosuojavastaava ja ilmoitettava hänen yhteystietonsa Tilaajalle. Tietosuojavastaava tai muu Palvelun tietoturvallisuudesta vastaava henkilö on velvollinen osallistumaan ilman eri veloitusta pyydettäessä Palvelun seurannan johtoryhmän tai muun vastaavan elimen kokouksiin.

(11) Toimittajan 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.

(12) Toimittaja sitoutuu ilman aiheetonta viivästystä ilmoittamaan Tilaajalle kaikista rekisteröityjen pyynnöistä, jotka koskevat voimassaolevan lainsäädännön sekä EU:n yleisen tietosuoja-asetuksen mukaisten rekisteröidyn oikeuksien käyttämistä.

Toimittaja sitoutuu avustamaan Tilaajaa asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, jotta Tilaaja pystyy täyttämään velvollisuutensa vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Henkilötietojen käsittelijänä Toimittaja ymmärtää, että näiden oikeuksien käyttämistä koskevat pyynnöt voivat edellyttää siltä avustamista rekisteröidylle tiedottamisessa ja vies-

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

(13) Tietoturvaloukkauksen sattuessa Toimittajan tulee avustaa Tilaajaa Tietosuoja-asetuksen 33 ja 34 artiklojen edellyttämän ilmoituksen tekemisessä valvontaviranomaiselle ja rekisteröidylle.

(14) Jos järjestelmässä on luonnollisten henkilöiden osoite- ja muita yhteystietoja, Toimittajalla on oltava valmius asettaa ja hallinnoida tietojen luovutuksia koskevia rajoituksia, jollaisia voi aiheutua esimerkiksi väestötietolain mukaisesta rekisteröidyn turvakiellosta. Toimittajan tulee pystyä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan Tilaajan vaatimalla tavalla. Rekisteröidyn henkilötietojen rajoittaminen ei saa johtaa muiden rekisterissä olevien luonnollisten henkilöiden henkilötietojen rajoittamiseen, ellei Tilaajan ja Toimittajan kesken kirjallisesti toisin sovita.

(15) Ellei toisin sovita, Toimittaja on velvollinen ylläpitämään luetteloa rekisteröityjen henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista. Luettelo on luovutettava pyydettäessä Tilaajalle. Tilaajan pyynnöstä Toimittajan on luovutettava luettelossa mainittuja tietoja Tilaajan pyytämässä laajuudessa Tilaajan yksilöimille kolmansille tahoille.

D. MUUT EHDOT

11. Palvelun seuranta ja tarkastaminen

(1) Palvelun seurannan ja tarkastamisen tavoitteena on Palvelun ylläpidon ja tietoturvallisuuden sekä niiden jatkuvan kehittämisen varmistaminen sekä Salassa pidettävän tiedon salassapidon toteutuminen.

(2) Tilaajalla on oikeus muuttaa, täydentää ja päivittää Toimittajalle antamiaan Tietoturvallisuusohjeita. Ohjeiden muutokset, täydennykset ja päivitykset voivat liittyä teknisiin tai organisatorisiin toimenpiteisiin, jotka koskevat tietoturvaa, henkilötietojen käsittelyä tai tietosuojaa. Toimittaja tekee tarvittavat muutostyöt Tilaajan ohjeiden mukaisesti. Jos Tilaajan ohjeiden muutokset aiheuttavat Toimittajalle olennaisia muutostöitä (yli yksi (1) henkilötyöpäivää), lisäkustannuksista sovitaan erikseen hintaliitteen mukaisesti. Toimittaja ja Toimittajan alihankkijat sitoutuvat noudattamaan näitä muutettuja, täydennettyjä tai päivitettyjä ohjeita.

(3) Toimittaja toimittaa Tilaajalle kuukausittain 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 Toimittaja raportoi välittömästi.
f. Tietomurron yritykset
g. Paikkaamattomat järjestelmähaavoittuvuudet sekä muut vastaavat poikkeamat, jotka ovat omiaan nostamaan riskiä Tilaajan Salassa pidettävien tietojen luottamuksellisuuden vaarantumiselle.

(4) Toimittaja sitoutuu reagoimaan viimeistään 72 tunnin kuluessa Tilaajan yhteydenotosta ja vastaamaan viimeistään yhden (1) viikon kuluessa Tilaajan tietoturvaa, henkilötietojen käsittelyä tai tietosuojaa koskeviin ilmoituksiin, reklamaatioihin tai muihin viesteihin, pois lukien EU:n yleisen tietosuoja-asetuksen mukaiset tietoturvaloukkaukset, joihin sovelletaan Sopimuksessa ja edellä tässä liitteessä määritettyjä määräaikoja.

(5) Toimittaja seuraa tämän Tietoturvaliitteen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Tilaajalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Tilaaja seuraa Palvelun turvallisuustason toteutumista yhteistyössä Toimittajan kanssa.

(6) Palvelun tarkastamiseksi suoritettava auditointimenettely on määritelty tämän Tietoturvaliitteen kohdassa 12.

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

(8) Osapuolet ymmärtävät, että Sopimusta ja tätä tietoturvallisuusliitettä tehtäessä tietosuojaa koskeva lainsäädäntö on muutostilassa. Jos kyseiseen lainsäädäntöön tai sitä tai sen tulkintaa koskeviin suosituksiin, ohjeistuksiin tai määräyksiin tulee muutoksia, jotka vaikuttavat Tilaajan asemaan tai velvollisuuksiin tai tässä liitteessä määriteltyihin velvollisuuksiin tai vastuisiin, tätä liitettä voidaan tarvittaessa niiltä osin tarkistaa. Jos tähän liitteeseen tehdään sellaisia muutoksia, joista aiheutuu Toimittajalle olennaisia lisäkustannuksia (yli yksi (1) henkilötyöpäivää), niiden korvaamisesta voidaan sopia erikseen Pääsopimuksen hintaliitteen hintojen mukaisesti. Toimittaja ja Toimittajan alihankkijat sitoutuvat noudattamaan kyseistä tarkistettua sopimusliitettä.

12. Auditointi

(1) Tilaajalla on oikeus auditoida Palvelu ja sen toimittaminen sekä siihen liittyvät Toimittajan järjestelmät. Auditoinnissa tilaajalla on oikeus käyttää ulkopuolista auditoijaa.

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

(3) Tilaajalla voi suorittaa auditoinnin enintään kerran kalenterivuodessa, ellei pakottavasta lainsäädännöstä, viranomaismääräyksistä tai tietoturvauhasta muuta johdu.

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

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

(6) Tilaaja vastaa auditoinnin järjestämisen kustannuksista. Mikäli kuitenkin auditoinnissa havaitaan merkittäviä puutteita Toimittajan turvallisuusjärjestelyissä tai tämän Tietoturvaliitteen noudattamisessa, vastaa auditoinnin kustannuksista Toimittaja.

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

(8) Toimittajan Pääsopimuksen tai tämän Tietoturvaliitteen vastaisista laiminlyönneistä tai virheistä aiheutuneet auditoinnissa ilmenneet puutteet ja virheet Toimittaja korjaa veloituksetta.

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

13. Sopimussakko

(1) Tilaajalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Tietoturvallisuusliitteen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Tilaajalla ei ole oikeutta sopimussakkoon vähäisistä rikkomuksista. Jos Toimittaja ei korjaa korjattavissa olevaa vähäistä rikkomusta, Tilaaja on kuitenkin oikeutettu sopimussakkoon.

(2) Sopimussakon määrä jokaista Tietoturvallisuusliitteen sopimusrikkomusta kohden on 30 % Palvelun kuukausiveloituksesta, kuitenkin vähintään 5.000 euroa ja enintään 50.000 euroa.

(3) Jos Toimittaja samalla teolla rikkoo useita tämän Tietoturvallisuusliitteen velvoitteita, katsotaan se kuitenkin vain yhdeksi sopimussakkoon oikeuttavaksi rikkomukseksi.

(4) Mikäli Toimittaja ei ole korjannut rikkomustaan 14 päivän kuluessa, katsotaan rikkomus uudeksi rikkomukseksi, jolloin Tilaaja on oikeutettu uuteen sopimussakkoon. Määräajan päättymisestä alkaa aina uusi tämän kohdan mukainen määräaika, ja rikkomus voidaan katsoa toistuvaksi uudeksi rikkomukseksi.

(5) Ennen sopimussakon perimistä Tilaajan tulee ilmoittaa Toimittajalle kirjallisesti tämän Tietoturvallisuusliitteen rikkomuksesta. Rikkomus käsitellään Tilaajan ja Toimittajan välisissä keskusteluissa.

(6) Tämän kohdan mukainen sopimussakko ei rajoita tai vähennä Tilaajan oikeutta vahingonkorvaukseen tai Pääsopimuksen mukaisiin muihin sanktioehtoihin.

(7) Tilaajalla on oikeus kuitata sopimussakkoa vastaava määrä Pääsopimuksen mukaisen Palvelun veloituksista.

14. Vahingonkorvaus

(1) Tämän tietoturvallisuusliitteen salassapitoa koskevien velvoitteiden rikkomiseen ei sovelleta Pääsopimuksen vastuunrajoituksia koskevia ehtoja.

(2) Tietosuoja-asetuksen 82 artiklan 5 kohdan mukaiseen perimisoikeuteen ei sovelleta Pääsopimuksen vastuunrajoituksia koskevia ehtoja.

(3) Mahdollinen sopimussakko ei rajoita Tilaajan oikeutta saada Toimittajalta vahingonkorvausta sopimusrikkomuksesta siltä osin, kun Tilaajalle aiheutunut vahinko ylittää sopimussakon määrän.