TIETOTURVALLISUUSLIITE

HELSINGIN KAUPUNKI

Helsingin kaupunki Tarkastusvirasto
Postiosoite PL 400 00099 HELSINGIN KAUPUNKI
Sähköposti tarkastusvirasto@hel.fi
Puhelin +358 9 310 1613
Y-tunnus 0201256-6

Sisällys

A. JOHDANTO

1. Määritelmät

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

(2) **Palvelu** tarkoittaa sitä palvelua, yhteistyötä tai muuta toimintaa, 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 kohdassa 3 (1) määriteltyä sopimusta liitteineen.

(4) **Suojattava 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 Tilaaja on merkinnyt salassa pidettäväksi tai kuuluvan Suojattaviin tietoihin tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin; tai
iv. kyseessä on muu tieto, jonka Sopijapuolet ovat sopineet kuuluvan Suojattaviin tietoihin; tai
v. 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) **Henkilötietojen käsittely** tarkoittaa Tietosuoja-asetuksen 4 artiklan mukaisesti toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaali-

sesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

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

2. Yhteyshenkilöt

(1) Tilaajan yhteyshenkilö tietoturvallisuusasioissa:
[*Nimi ja yhteystiedot*]

(2) Toimittajan yhteyshenkilö tietoturvallisuusasioissa:
[*Nimi ja yhteystiedot*]

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

3. Tietoturvallisuusliitteen tausta ja tarkoitus

(1) Sopijapuolet ovat tehneet Pääsopimuksen [*sopimuksen kohde, sopimusnumero, allekirjoituspäivämäärä*], jolla Sopijapuolet ovat sopineet Palvelun tuottamisesta.

(2) Toimittaja on valittu kilpailutuksen [*XX]* perusteella Helsingin kaupungin hallinnon ja talouden lakisääteisen tilintarkastuksen ja eräiden erityistoimeksiantojen suorittajaksi.

Toimittaja käsittelee Tilaajan henkilötietoja lakisääteisen tilintarkastustehtävän toteuttamisen yhteydessä. Tilintarkastus tehtävän toteuttamiseksi Toimittajalla annetaan tehtävänsä suorittamisen edellyttämässä laajuudessa pääsy Tilaajan järjestelmiin ja Toimittaja kerää ja tallentaa henkilötietoja tarvittaessa myös omiin järjestelmiin. Tilaajan rekisterissä on henkilötietoja esimerkiksi Tilaajan työntekijöistä, viranhaltijoista, luottamushenkilöistä, kuntalaisista, kunnan sopimus- ja yhteistyökumppaneista ja kunnan asiakkaista. Käsittelyn kohteena ovat Tilaajan hallussa olevat henkilötiedot, joiden käsittely on tarpeen tilintarkastustehtävän toteuttamiseksi sisältäen muun muassa nimiä, osoitetietoja ja henkilötunnuksia.

(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.

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. Toimittaja vastaa siitä, että Tilaajan tämän liitteen mukainen Tilaajan tarkastusoikeus voidaan ulottaa myös Toimittajan Alihankkijoihin.

(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 (Pääsopimuksen liite 3) ja Tilaajan tietoturvallisuusohjeita (Pääsopimuksen liite 3.1) 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) 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.

(5) Tilaaja laatii tarvittaessa tietojärjestelmäselosteen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annetun asetuksen 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 Suojattavien 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 tietoturvaan ja 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) 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 Suojattavia tietoja tai pääsevät järjestelmiin, jotka sisältävät Suojattavia tietoja.

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

(3) 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, hyvää tietojen käsittelytapaa, Tietosuoja-asetusta sekä muuta tietojen suojaamista ja tietosuojaa koskevaa lainsäädäntöä Palvelun tuottamisessa.

(2) Tilaajalla on oikeus luokitella Suojattavat tiedot niiden suojaustarpeen perusteella. Toimittaja käsittelee Tilaajan Suojattavia tietoja niiden turvallisuusluokkien edellyttämällä tavalla.

6.3 Pääsy tiloihin

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

(2) Mikäli Palvelua suoritetaan 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 Suojattaviin tietoihin tai niitä sisältäviin järjestelmiin kohdan 6.4 mukaisesti, saavat oleskella Tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Suojattavia tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

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

6.4 Pääsy järjestelmiin ja tietoihin

(1) Toimittaja vastaa siitä, että Suojattavia tietoja annetaan, sellaisia tietoja pääsee käsittelemään tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain sellaisille 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 Tietoturvallisuusliitteen 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. Tarkastamisesta vastaa kunkin järjestelmän osalta se Sopijapuoli, joka ylläpitää ja hallinnoi kyseisen järjestelmän käyttöoikeuksia. 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) Toimittaja ilmoittaa Tilaajalle Palveluun liittyvistä tietoturvapoikkeamista kirjallisesti välittömästi saatuaan ne tietoonsa. Ilmoitusvelvollisuus koskee ainakin toteutuneita tietovuotoja/-murtoja, tietomurron yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia sekä muita vastaavaa poikkeamia, jotka ovat omiaan nostamaan riskiä Tilaajan Salassa pidettävien tietojen luottamuksellisuuden vaarantumiselle.

(2) Lisäksi Toimittaja ilmoittaa 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 välittömästi Toimittajan saatua niistä tiedon.

(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.

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

(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 yhteisesti 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) Palvelujen muuttamista tai laajentamista koskevan suunnittelun alkuvaiheessa tarkistetaan tietoturvallisuuteen liittyvät vaatimukset. Tilaaja määrittelee kyseiset vaatimukset.

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

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

(4) Tämän Tietoturvallisuusliitteen yhteyshenkilöt vastaavat tämän liitteen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan tarvittaessa yhteyshenkilöiden kesken.

(5) 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 Suojattavaa tietoa.

(2) Tilaaja noudattaa julkisyhteisönä julkisuuslaissa sekä muussa lainsäädännössä olevia salassapitoa, julkisuutta ja yksityisyydensuojaa koskevia säännöksiä. Tällä Tietoturvallisuusliitteellä 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) sen kumoamiseen saakka, Tietosuojalaki sen voimaan tulosta alkaen
- EU:n tietosuoja-asetus (EU 2016/679)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki yksityisyyden suojasta työelämässä (759/2004)

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

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

(6) Toimittaja käsittelee Suojattavia tietoja vain Palvelun tuottamisen edellyttämässä laajuudessa. Toimittaja antaa Suojattavia tietoja vain niille henkilöille, jotka tar-

vitsevat Suojattavia tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Toimittaja sitoutuu antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Suojattavien 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, ellei lainsäädännöstä muuta johdu.

(9) Pääsopimuksen päättyessä Toimittaja ja sen Alihankkijat palauttavat Tilaajan Suojattavaa tietoa sisältävän aineiston ja muun Tilaajan osoittaman Tilaajalle kuuluvan aineiston sekä hävittävät taltioillaan olevan tietoaineiston ja kopiot. Toimittaja vastaa siitä, että Tilaajan aineisto on erillään tai erotettavissa Toimittajan muusta aineistosta. Aineistoa ei saa hävittää, mikäli Tilaaja, laki tai viranomaisten määräykset vaativat sen säilyttämistä.

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

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 ellei lainsäädännöstä muuta johdu.

Toimittaja ei saa käsitellä, 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.

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

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

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

(6) Mikäli Tietosuoja-asetus edellyttää tietosuojavastaavan nimeämistä, 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.

(7) 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.

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

(9) 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 viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa ja/tai henkilötietojen siirtämisessä järjestelmästä toiseen.

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

(11) Mikäli toimittaja käsittelee luonnollisten henkilöiden osoite- ja muita yhteystietoja omassaan tai Alihankkijansa järjestelmässä, 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.

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 Suojattavan 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 Pääsopimuksen hintaliitteen mukaisesti. Toimittaja ja Toimittajan Alihankkijat sitoutuvat noudattamaan näitä muutettuja, täydennettyjä tai päivitettyjä ohjeita.

(3) Toimittaja toimittaa Tilaajalle tarvittaessa 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 Tietosuoja-asetuksen mukaiset tietoturvaloukkaukset, joihin Toimittaja reagoi kohdan 7 (1) mukaisesti välittömästi saatuaan ne tietoonsa.

(5) Toimittaja seuraa tämän Tietoturvallisuusliitteen 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 Tietoturvallisuusliitteen 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) Tilaaja voi suorittaa auditoinnin enintään kerran kalenterivuodessa, ellei pakottavasta lainsäädännöstä, viranomaismääräyksistä tai tietoturvauhasta muuta johdu. Tilaajalla on aina tietoturvaloukkausten yhteydessä oikeus suorittaa auditointi.

(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 Tietoturvallisuusliitteen 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. Vahingonkorvaus

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

(2) Jos Tilaaja on Tietosuoja-asetuksen 82 artiklan 4 kohdan mukaisesti maksanut rekisteröidylle korvauksen aiheutuneesta vahingosta, ja jos kyseisen vahingon voidaan katsoa aiheutuneen Toimittajan tai sen palveluksessa olevan henkilön tai Toimittajan Alihankkijan menettelyn tai laiminlyönnin seurauksena tai johdosta, on Toimittaja velvollinen korvaamaan Tilaajalle Tilaajan maksaman korvauksen täysimääräisesti sovittujen vastuunrajoitusten estämättä.