Kaupunginkanslia
Oikeuspalvelut 5.6.2019

TIETOTURVALLISUUSLIITE

HELSINGIN KAUPUNKI
Kaupunginkanslia (Ahjo-Hanke)

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

Sisällys

A. JOHDANTO

1. Määritelmät

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

(2) **Henkilötieto** tarkoittaa Rekisterinpitäjän hallussa olevia Rekisteröityyn liittyviä tietoja, jotka Käsittelijä on saanut käsiteltäväksi ennen tai jälkeen tämän Tietoturvallisuusliitteen allekirjoittamisen.

(3) **Käsittelijä** tai **Toimittaja** tarkoittaa Henkilötietolainsäädännön mukaista Henkilötietojen käsittelijää, joka käsittelee Henkilötietoja Rekisterinpitäjän puolesta ja lukuun.

(4) **Ohjelmisto** tarkoittaa sitä ohjelmistoa, josta Tilaaja ja Toimittaja ovat sopineet Pääsopimuksessa.

(5) **Pääsopimus** tarkoittaa Sopijapuolten välistä sopimusta (mukaan lukien sen liitteet), jonka mukaisesti Käsittelijä tarjoaa Internet-videoiden tuottamiseen, jakamiseen ja julkaisuun tarkoitettua, Liitteessä A tarkemmin kuvattua, ohjelmistoa SaaS-Ohjelmistona Rekisterinpitäjälle.

(6) **Rekisteröity** tarkoittaa tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä, jonka Henkilötietoja käsitellään Käsittelijän toimesta tämän Tietoturvallisuusliitteen ja Pääsopimuksen mukaisesti.

(7) **Rekisterinpitäjä** tai **Tilaaja** tarkoittaa Henkilötietolainsäädännön mukaista rekisterinpitäjää, joka määrittelee Henkilötietojen käsittelyn tarkoitukset ja keinot.

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

(9) **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.

(10) **Tietoturvallisuusliite** tarkoittaa tätä asiakirjaa, jolla Sopijapuolet sopivat Henkilötietojen käsittelystä.

2. Yhteyshenkilöt

(1) Tilaajan yhteyshenkilö tietoturvallisuusasioissa:

(2) Toimittajan yhteyshenkilö tietoturvallisuusasioissa:

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

3. Tietoturvallisuusliitteen tausta ja tarkoitus

(1) Sopijapuolet ovat tehneet Pääsopimuksen, jolla Sopijapuolet ovat sopineet Toimittajan tarjoavan Internet-videoiden tuottamiseen, jakamiseen ja julkaisuun tarkoitettua Ohjelmistoa SaaS-Ohjelmistona.

(2) Mikäli Ohjelmistoon sisältyy Henkilötietojen käsittelyä, Sopijapuolet sopivat tässä Tietoturvallisuusliitteessä ja sen liitteessä A 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 sekä liitteessä A määritellään Sopijapuolten välillä noudatettavat Henkilötietoja koskevat turvallisuusjärjestelyt Pääsopimuksen sisältämän Ohjelmiston tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Sopijapuolten välisessä yhteistyössä.

(4) 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.

(5) 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 saa käyttää Henkilötietojen käsittelyyn alihankkijoita.

(2) Tämän Tietoturvallisuusliitteen Voimaantulopäivänä Käsittelijän käyttämät alihankkijat on listattu Liitteessä A. Toimittajan on tiedotettava Tilaajalle kirjallisesti kaikista muutoksista, jotka koskevat Henkilötietojen käsittelijöinä toimivien alihankkijoiden lisäämistä tai vaihtamista, ja annettava Tilaajalle mahdollisuus vastustaa tällaisia muutoksia. Tilaajalla on oikeus vastustaa Toimittajan Henkilötietojen käsittelijänä toimivaa uutta alihankkijaa ainoastaan perustellusta syystä. Mikäli Tilaaja vastustaa uutta alihankkijaa, Sopijapuolet sitoutuvat keskustelemaan asiasta ja pyrkivät yhteistyössä löytämään asiaan ratkaisun. Mikäli asiaa ei saada ratkaistua, Tilaajalla on oikeus irtisanoa tämä Tietoturvallisuusliite sekä Pääsopimus välittömästi ilmoittamalla siitä kirjallisesti Käsittelijälle 30 päivän kuluessa keskusteluiden päättymisestä. Jollei Rekisterinpitäjä vastusta uutta alihankkijaa 30 päivän kuluessa Käsittelijän ilmoituksesta tai irtisano tätä Tietoturvallisuusliittettä sekä Pääsopimusta 30 päivän kuluessa asiaa koskevien keskusteluiden päättymisestä, Rekisterinpitäjän katsotaan hyväksyneen ilmoitetun alihankkijan käytön. Pääsopimuksen nojalla suoritetut maksut irtisanomisen jälkeiseltä ajalta palautetaan.

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

(4) Tässä Tietoturvallisuusliitteessä Toimittajan henkilöstölle asetettavia velvoitteita sovelletaan myös Alihankkijan Ohjelmiston tuottamiseen osallistuvaan henkilöstöön.

(5) Käsittelijällä on oikeus käyttää konserniyhtiöitään Henkilötietojen käsittelyssä.

B. TIETOTURVALLISUUS JA SALASSAPITO

5. Sopijapuolten yleiset velvoitteet

(1) Rekisterinpitäjä:

a. vastaa Henkilötietojen siirrosta Käsittelijälle Pääsopimuksen mukaisia tarkoituksia varten;
b. vastaa siitä, että sillä on oikeus siirtää Henkilötiedot Käsittelijälle;
c. käsittelee Henkilötietoja henkilötietolainsäädännön sekä hyvän tietosuojakäytännön mukaisesti;
d. on oikeutettu antamaan kohdan 5.4 mukaisesti Käsittelijälle tarkempia Henkilötietojen käsittelyä koskevia ohjeita, joiden tulee olla henkilötietolainsäädännön mukaisia;
e. päättää Henkilötietojen käytöstä ja käsittelystä;
f. hallinnoi Henkilötietoja;
g. vastaa siitä, että sen suorittama Henkilötietojen käsittely on lainmukaista; ja
h. vastaa siitä, että Henkilötietoja Rekisterinpitäjän puolesta pyytävällä taholla on oikeus saada pääsy Henkilötietoihin.

(2) Toimittaja ja sen alihankkija noudattavat tätä Tietoturvallisuusliitettä Ohjelmiston tuottamisessa. Lisäksi Toimittaja ja sen alihankkija noudattavat Toimittajan sisäisiä tietoturvallisuusohjeita.

(3) Käyttämällä Pääsopimuksen mukaisia Ohjelmistoa Rekisterinpitäjä antaa Käsittelijälle ohjeet käsitellä ja käyttää Henkilötietoja siinä määrin kuin on tarpeen Pääsopimuksen ehtojen täyttämiseksi. Käsittelijä käsittelee Henkilötietoja Liitteessä A kuvatusti, ellei henkilötietolainsäädäntö toisin edellytä. Allekirjoittamalla tämän Tietoturvallisuusliitteen Rekisterinpitäjä ohjeistaa Käsittelijää käsittelemään Henkilötietoja Liitteessä A kuvatusti.

(4) Mikäli Rekisterinpitäjä haluaa antaa Käsittelijälle kohtuullisia täydentäviä ohjeita Henkilötietojen käsittelystä, tulee ohjeet toimittaa kirjallisesti. Ohjeet tulevat Käsittelijää sitovaksi Käsittelijän hyväksyttyä ne kirjallisesti. Mikäli Käsittelijä ei pysty noudattamaan edellä mainittuja täydentäviä ohjeita, Sopijapuolet pyrkivät tällöin yhteistyössä löytämään ratkaisun täydentäviin ohjeisiin liittyen. Mikäli täydentäviä ohjeita koskevaa asiaa ei saada ratkaistua kahden (2) kuukauden kuluessa Rekisterinpitäjän täydentävien ohjeiden toimittamisesta, on kummallakin Sopijapuolella oikeus irtisanoa tämä Tietoturvallisuusliite sekä Pääsopimus välittömästi. Pääsopimuksen nojalla suoritetut maksut irtisanomisen jälkeiseltä ajalta palautetaan. Käsittelijällä on oikeus laskuttaa erikseen kirjallisesti

sovittujen täydentävien ohjeiden toteuttamisesta aiheutuvat kohtuulliset lisäkustannukset ja lisätyöt Rekisterinpitäjältä.

(5) Rekisterinpitäjän antamien ohjeiden tulee olla Henkilötietolainsäädännön ja muun pakottavan lainsäädännön sekä hyvän tietojenkäsittelytavan mukaisia. Rekisterinpitäjä on vastuussa Henkilötietojen täsmällisyydestä, eheydestä, laadusta ja lainmukaisuudesta sekä siitä, että se on lainmukaisesti ilmoittanut Rekisteröidyille Henkilötietojen käsittelystä.

(6) Käsittelijä ei vastaa Henkilötietojen asianmukaisesta, ohjeistusten ja Henkilötietolainsäädännön mukaisesta käsittelystä Rekisterinpitäjän lukuun toimivien henkilöiden, kuten esimerkiksi Ohjelmiston käyttäjien, toimesta.

(7) Toimittaja vastaa siitä, ettei Henkilötietojen luottamuksellisuus, saatavuus tai eheys vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Tietoturvallisuusliitteen tai Pääsopimuksen vastaisen toiminnan johdosta.

(8) Toimittaja vastaa siitä, että sen tuottama Ohjelmisto on vikasietokykyinen ja Ohjelmiston tallennetut tiedot pystytään palauttamaan nopeasti fyysisen tai teknisen vian sattuessa liitteessä A kuvatusti.

(9) 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.

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

(11) Käsittelijä ei siirrä Henkilötietoja Euroopan talousalueelta sen ulkopuolelle tai mahdollista pääsyä kyseisiin Euroopan talousalueella oleviin Henkilötietoihin Euroopan talousalueen ulkopuolelta, ellei Rekisterinpitäjä nimenomaisesti niin pyydä. Mikäli Rekisterinpitäjä esittää tällaisen pyynnön, Sopijapuolet sopivat kirjallisesti erikseen siirron toteuttamisesta ja kustannuksista.

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

6. Toimittajan tietoturvallisuus

(1) Toimittajan tekniset ja organisatoriset toimenpiteet on kuvattu Liitteessä A. Rekisterinpitäjä vastaa siitä, että se tarkistaa ja hyväksyy Liitteen A mukaiset kuvaukset Voimaantulopäivänä ja että kuvatut toimenpiteet vastaavat Voimaantulopäivänä riittävää turvallisuustasoa ottaen huomioon Henkilötietojen käsittelyn tarkoitus ja luonne. Liitteen A mukaiset kuvaukset ovat riippuvaisia teknisestä kehityksestä, joten niiden sisältö ja laajuus voivat muuttua. Tästä syystä Käsittelijällä on oikeus yksin päivittää Liitteen A mukaisia kuvauksia ja implementoida vaihtoehtoisia Henkilötietolainsäädännön mukaisia teknisiä ja organisatorisia toimenpiteitä Liitteessä A kuvattujen toimenpiteiden tilalle edellyttäen, että tällaiset muutokset eivät heikennä tietoturvan tasoa.

(2) Toimittaja informoi Tilaajaa Ohjelmiston tietoturvallisuudesta ja muista vaatimustenmukaisuuteen liittyvistä seikoista, mikäli niissä tapahtuu muutoksia sopimuksen allekirjoittamisen jälkeen. Tämän Tietoturvallisuusliitteen mukaiset ilmoitukset toimitetaan tämän liitteen kohdan 2 mukaiselle yhteyshenkilölle sähköpostitse. Rekisterinpitäjä on yksin vastuussa siitä, että sen yhteystiedot ovat kulloinkin oikeita ja ajan tasalla.

(3) Toimittaja määrittelee organisaatiossaan tietoturvallisuuteen liittyvät tehtävät ja vastuut sekä nimeää henkilöt Ohjelmistoon liittyvistä tietoturva-asioista tiedottamiseen ja tietoturvapoikkeamista raportointiin.

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

(5) Tietoturvallisuuspäivityksien, käyttöoikeuksien valvonnan, käyttöoikeuksien hallinnan ja muiden vastaavien tietoturvallisuuteen liittyvien käytäntöjen osalta sovelletaan Pääsopimuksessa tai Liitteessä A sovittuja käytäntöjä.

6.1 Henkilöstöturvallisuus ja turvallisuusselvitykset

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

6.2 Tietoaineistoturvallisuus

(1) Toimittaja noudattaa henkilötietolain edellyttämää hyvää tietojen käsittelytapaa, Tietosuoja-asetusta sekä muuta tietojen suojaamista ja tietosuojaa koskevaa lainsäädäntöä Ohjelmiston tuottamisessa Liitteessä A kuvatusti.

(2) Toimittaja käsittelee Tilaajan tietoaineistoja Liitteessä A kuvatulla tavalla.

6.3 Pääsy tiloihin

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

(2) Mikäli Ohjelmistoa tuotetaan Toimittajan tai sen Alihankkijan tiloissa, Toimittajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. erityistilanteiden varalta.

(3) Henkilöt, joille ei ole myönnetty oikeutta Henkilötietoihin tai niitä sisältäviin järjestelmiin kohdan 6.4 mukaisesti, saavat oleskella Tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Henkilötietoja 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 Henkilötietoja annetaan, sellaisia tietoja pääsee käsittelemään tai pääsy Henkilötietoja 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 salassapitositoumuksen ennen kuin hän aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin.

7. Tietoturvaloukkausten käsittely

(1) Ohjelmistoon liittyvistä tietoturvapoikkeamista Toimittaja on velvollinen kirjallisesti ilmoittamaan Tilaajalle ilman aiheetonta viivytystä saatuaan sen tietoonsa. Ilmoitusvelvollisuus koskee ainakin toteutuneita tietovuotoja/-murtoja, tietomurron yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia sekä muita vastaavaa poikkeamia, jotka ovat omiaan nostamaan riskiä Tilaajan Henkilötietojen luottamuksellisuuden vaarantumiselle (siltä osin, kuin ne ovat Käsittelijän hallussa ja tiedossa).

(2) Lisäksi Toimittaja sitoutuu ilmoittamaan Tilaajalle ilman aiheetonta viivytystä muista Toimittajan tuottaman Ohjelmiston olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia Henkilötietojen luottamukselliselle käsittelylle tai sellaisten henkilöiden asemaan ja oikeuksiin, joiden henkilötietoja Toimittaja käsittelee.

(3) Toimittajan on annettava Tilaajalle vähintään seuraavat tiedot tietoturvaloukkauksesta (siltä osin, kuin ne ovat Käsitteljän hallussa ja tiedossa):

- 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 Ohjelmiston tuottamiseen liittyvissä häiriötilanteissa toimimisen sekä niistä ilmoittamisen osalta.

(5) Toimittaja huolehtii häiriötilanteiden hallinnasta Pääsopimuksen ja omien käytäntöjensä mukaisesti siten, että ongelman rajaus ja korjaus suoritetaan.

(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) Käsittelijällä on oikeus omatoimisesti ryhtyä tarvittaviin toimiin Henkilötietojen turvaamiseksi ja Tietoturvaloukkauksen vaikutusten minimoimiseksi.

(9) Rekisterinpitäjän on ilmoitettava Käsittelijälle viipymättä, jos Rekisterinpitäjän tietoon tulee Tietoturvaloukkaus, joka koskee Henkilötietoja. Rekisterinpitäjän on lisäksi ilmoitettava Käsittelijälle viipymättä tilien tai tunnusten mahdollisista väärinkäytöksistä tai Ohjelmistoon liittyvistä turvallisuusongelmista.

(10) Jos Käsittelijä tarvitsee Tietoturvaloukkaustilanteessa tietoja voidakseen täyttää tämän Tietoturvallisuusliitteen ja Henkilötietolainsäädännön mukaiset velvollisuutensa, Rekisterinpitäjän on annettava ne Käsittelijälle ilman aiheetonta viivytystä.

8. Tietoturvallisuuteen liittyvä muutoshallinta ja kehittäminen

(1) Ohjelmistoon kohdistuvissa muutoksissa toimitaan Pääsopimuksessa määritellyn muutoshallintamenettelyn tai Toimittajan omien prosessien mukaisesti.

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

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

(4) Tähän Tietoturvallisuusliitteeseen tehtävät muutokset tulee tehdä kirjallisesti ja molempien Sopijapuolten tulee vahvistaa ne alle, lukuun ottamatta Liitteen A muutoksia. Tämän Tietoturvallisuusliitteen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

9. Salassapito

(1) Sopijapuolet noudattavat tässä Tietoturvallisuusliitteessä määriteltyjä turvallisuusjärjestelyitä aina Toimittajan tai sen Alihankkijan käsitellessä Henkilötietoa.

(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) Toimittaja pitää salassa kaikki Henkilötiedot. Toimittaja käsittelee henkilötietoja ainoastaan Sopimuksen mukaisiin tarkoituksiin.

(4) Toimittaja säilyttää ja käsittelee Henkilötietoja siten, että ne pysyvät vain niiden henkilöiden hallussa, joilla on oikeus Henkilötietoihin, eivätkä ne joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

(5) Toimittaja käsittelee Henkilötietoja vain Pääsopimuksen mukaisten velvoitteiden täyttämisen edellyttämässä laajuudessa. Toimittaja antaa Henkilötietoja vain niille henkilöille, jotka tarvitsevat Henkilötietoja työtehtävissään. Toimittaja sitoutuu antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Henkilötietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin.

(6) Toimittaja vastaa henkilöstönsä salassapitositoumuksista kohdan 6.4(3) mukaisesti.

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

(8) Ennen Pääsopimuksen päättymistä Tilaajalla on mahdollisuus palauttaa ja/tai poistaa Henkilötiedot Ohjelmistosta. Siltä osin, kuin tämä ei ole teknisesti mahdollista, Käsittelijä voi avustaa Henkilötietojen palauttamisessa ja poistamisessa. Henkilötietojen palauttaminen ja poistaminen on kuvattu tarkemmin Liitteessä A. Henkilötietoja ei saa hävittää, mikäli Toimittajaan soveltuva laki tai viranomaisten määräykset vaativat sen säilyttämistä.

(9) Tämän Tietoturvallisuusliitteen mukainen Henkilötietoja koskeva 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 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 tarpeen Pääsopimuksen mukaisten velvollisuuksien täyttämiseksi ja vain siihen saakka kuin Pääsopimuksella määrätään tai Toimittajan avustamisvelvollisuus on päättynyt Tietosuoja-asetuksen mukaisesti. Toimittajalla ei ole oikeutta käyttää saamiaan henkilötietoja omassa toiminnassaan, käsitellä niitä tämän Tietoturvallisuusliitteen vastaisesti, yhdistää henkilötietoja muuhun hallussaan olevaan aineistoon eikä luovuttaa niitä. Toimittajalla on oikeus luovuttaa Henkilötietoja konserniyhtiöilleen ja muille Alihankkijoilleen Pääsopimuksen velvoitteiden täyttämiseksi. Henkilötietojen palauttaminen ja poistaminen on kuvattu tarkemmin Liitteessä A.

(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, jos palvelimien sijaintipaikka muuttuu.

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

(6) Toimittajan on tarvittaessa avustettava Tilaajaa Tietosuoja-asetuksen 35 artiklan mukaisen vaikutusten arvioinnin tekemisessä ja 36 artiklan mukaisen

ennakkokuulemisen toteuttamisessa. Toimittajalla on oikeus laskuttaa Tilaajaa kyseisestä työstä erikseen sovittavan hinnan mukaisesti.

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

(8) Käsittelijä ilmoittaa Rekisterinpitäjälle asianmukaisesti, siinä määrin kuin laillisesti mahdollista, mikäli se saa Rekisteröidyltä pyynnön saada pääsy häntä koskeviin Henkilötietoihin tai pyynnön rajoittaa, korjata, muuttaa tai poistaa Rekisteröidyn Henkilötiedot. Rekisterinpitäjällä on ensisijainen velvollisuus vastata suoraan Rekisteröidylle. Käsittelijä voi tarvittaessa auttaa Rekisterinpitäjää pyyntöihin vastaamisessa Rekisterinpitäjän pyynnön ja/tai ohjeistuksen perusteella.

(9) Ohjelmiston luonteesta johtuen, Käsittelijä ei tarkastele Rekisterinpitäjän Ohjelmistossa olevaa sisältöä eikä siten ole tietoinen Rekisteröidyistä tai Henkilötietojen sisällöstä tai luonteesta. Tästä johtuen kaikki Rekisterinpitäjän Ohjelmistossa olevaan sisältöön liittyvät pyynnöt ohjataan ensisijaisesti Rekisterinpitäjälle. Rekisteröidyn pyynnöstä Rekisterinpitäjä poistaa itsenäisesti Henkilötiedot Ohjelmistosta Pääsopimuksen voimassaoloaikana. Mikäli tarpeen, Käsittelijän on kohtuullisissa määrin mahdollista auttaa Rekisterinpitäjää Henkilötietojen poistamisessa. Henkilötietojen palauttaminen ja poistaminen Ohjelmistosta on kuvattu tarkemmin Liitteessä A.

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

(11) 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. Tilaajalla on ensisijainen velvollisuus rajoittaa Henkilötietojen käsittelyä järkestelmässä. Käsittelijän on kohtuullisissa määrin mahdollista auttaa Rekisterinpitäjää Henkilötietojen käytön rajoittamisessa.

D. MUUT EHDOT

11. Ohjelmiston seuranta ja tarkastaminen

(1) Seurannan ja tarkastamisen tavoitteena on Ohjelmiston ylläpidon ja tietoturvallisuuden sekä niiden jatkuvan kehittämisen varmistaminen sekä Henkilötietojen salassapidon toteutuminen.

(2) Mikäli Rekisterinpitäjä haluaa antaa Käsittelijälle kohdassa 5.3 mainittuja ohjeita täydentäviä ohjeita Henkilötietojen käsittelystä, noudatetaan kohdassa 5.4 sovittua menettelyä.

(3) Jos Tilaajan ohjeiden muutokset aiheuttavat Toimittajalle olennaisia muutostöitä (yli yksi (1) henkilötyöpäivää), lisäkustannuksista sovitaan erikseen. Toimittajalla on oikeus laskuttaa alle yhden henkilötyöpäivän muutostöistä syntyvät veloitukset ilman erillistä sopimusta voimassa olevan hinnaston mukaisesti. Toimittajalla on laskutusoikeus vain Tilaajan etukäteen kirjallisesti hyväksymien lisätöiden osalta. Toimittaja Toimittaja ja Toimittajan alihankkijat sitoutuvat noudattamaan näitä kohdassa 5.4 sovitun menettelyn mukaisesti muutettuja, täydennettyjä tai päivitettyjä ohjeita.

(4) Rekisterinpitäjän antamien ohjeiden tulee olla Henkilötietolainsäädännön ja muun pakottavan lainsäädännön sekä hyvän tietojenkäsittelytavan mukaisia. Rekisterinpitäjä on vastuussa Henkilötietojen täsmällisyydestä, eheydestä, laadusta ja lainmukaisuudesta sekä siitä, että se on lainmukaisesti ilmoittanut Rekisteröidyille Henkilötietojen käsittelystä.

(5) Toimittaja toimittaa Tilaajalle tarvittaessa tai Tilaajan pyynnöstä jälkikäteen tietoturvaraportin, josta tulee ilmetä ainakin alla listatut asiat. Tietoturvaraportti ei saa johtaa Toimittajan salassapitoa koskevien velvoitteiden rikkomiseen kolmansia osapuolia kohtaan eikä vaarantaa Toimittajan tietoturvaa.

   a. Liitteeseen A tehtävät muutokset
   b. Tehdyt tietoturvallisuustoimet (haavoittuvuuksien paikkaukset, versiopäivitykset, turvaohjelmistojen asennukset jne.) Toimittajan omien käytäntöjen mukaisesti
   c. Paikkaamattomat järjestelmähaavoittuvuudet sekä muut vastaavat poikkeamat, jotka ovat omiaan nostamaan riskiä Tilaajan Henkilötietojen luottamuksellisuuden vaarantumiselle.

(6) Toimittaja sitoutuu reagoimaan ilman aiheetonta viivytystä 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.

(7) Toimittaja seuraa tämän Tietoturvallisuusliitteen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat sekä aloittaa korjaustoimet omien prosessiensa mukaisesti. Tilaaja seuraa Ohjelmiston turvallisuustason toteutumista.

(8) Tietoturvan tarkastamiseksi suoritettava auditointimenettely on määritelty tämän Tietoturvallisuusliitteen kohdassa 12.

(9) Tilaaja ei vastaa Ohjelmiston seurannan ja tarkastamisen perusteella tehtävistä korjauksista aiheutuvista kustannuksista. Tilaajalla on oikeus vaatia ilman veloitusta tehtäviä korjauksia ainoastaan, mikäli järjestelyn todetaan olevan sopimuksen ja tämän liitteen vastainen. Muista korjauksista Toimittaja veloittaa tapauskohtaisesti erikseen sovittavalla tavalla.

(10) Osapuolet ymmärtävät, että 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 Sopijapuolen 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. Toimittajalla on oikeus laskuttaa alle yhden henkilötyöpäivän muutostöistä syntyvät veloitukset ilman erillistä sopimusta. Toimittajalla on laskutusoikeus vain Tilaajan etukäteen kirjallisesti hyväksymien lisätöiden osalta. Toimittaja ja Toimittajan alihankkijat sitoutuvat noudattamaan kyseistä tarkistettua sopimusliitettä.

12. Auditointi

(1) Rekisterinpitäjällä on oikeus tarkastaa tähän Tietoturvallisuusliitteeseen liittyen Käsittelijän pääkonttori ja Henkilötietojen käsittelyyn liittyvä dokumentaatio ilmoittamalla Käsittelijälle asiasta kohtuullisessa ajassa etukäteen. Tarkastuksen tulee tapahtua Käsittelijän normaalina toimistotyöaikana eikä se saa aiheuttaa haittaa Käsittelijän toiminnalle. Käsittelijällä on oikeus hyväksyä tarkastuksen suorittava taho ja kyseisen tahon on allekirjoitettava Käsittelijän salassapitositoumus ennen tarkastusta. Käsittelijällä on oikeus hyväksyä tarkastuksen suorittava taho, mutta Käsittelijä ei voi perusteettomasti vastustaa tarkastuksen suorittavaa tahoa.

(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 Ohjelmisto 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. Toimittajalla on oikeus hyödyntää raporttia täysimääräisesti toiminnassaan.

(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, jotka ovat Pääsopimuksen, tämän Tietoturvallisuusliitteen tai tietosuojaa ja tietoturvaa koskevan lainsäädännön vastaisia ilman aiheetonta viivytystä. Olennaiset Pääsopimuksen, tämän Tietoturvallisuusliitteen tai tietosuojaa ja tietoturvaa koskevan lainsäädännön vastaiset puutteet, jotka muodostavat ilmeisen uhan tietoturvallisuudelle, on Toimittajan korjattava ilman tarpeetonta viivästystä. Mikäli Toimittaja ei korjaa puutteita, on Tilaajalla oikeus irtisanoa Pääsopimus päättymään välittömästi.

(8) Toimittajan Pääsopimuksen tai tämän Tietoturvallisuusliitteen tai Toimittajaa koskevan tietosuojaa ja tietoturvaa koskevan lainsäädännön vastaisista laiminlyönneistä tai virheistä aiheutuneet auditoinnissa ilmenneet puutteet ja virheet Toimittaja korjaa veloituksetta. Mikäli Toimittaja ei korjaa puutteita, on Tilaajalla oikeus irtisanoa Pääsopimus päättymään välittömästi.

(9) Tilaajalla on oikeus luovuttaa muille viranomaisille tieto tarkastuksen lopputuloksesta, mikäli luovuttaminen perustuu pakottavaan lainsäädäntöön.

13. Sopimuksenpurkuehto

(1) Oikeus sopimuksenpurkuun syntyy, mikäli Tilaaja on antanut Toimittajalle kirjallisen ilmoituksen tämän Tietoturvallisuusliitteen soveltamisalaan kuuluvasta olennaisesta tai toistuvasta sopimusrikkomuksesta ja tämä ei ole korjannut menettelyään 30 vuorokauden kuluessa ilmoituksesta.

(2) Jos Palvelussa olevaa virhettä ei korjata määräaikaan mennessä, Pääsopimus voidaan purkaa Tilaajan toimesta yksipuolisesti.

(3) Mikäli Toimittaja ei ole korjannut rikkomustaan 30 päivän kuluessa ensimmäisen 30 vuorokauden määräajan päättymisestä, katsotaan rikkomus toistuvaksi rikkomukseksi.

(4) Ennen sopimuksen purkamista Sopijapuolen tulee ilmoittaa liitettä rikkoneelle Sopijapuolelle kirjallisesti tämän Tietoturvallisuusliitteen rikkomuksesta. Rikkomus käsitellään Tilaajan ja Toimittajan välisissä keskusteluissa.

14. Vahingonkorvaus

(1) Sopijapuolella on oikeus saada tämän sopimuskohdan 14 mukaisesti korvaus välittömästä vahingosta, joka sille on aiheutunut toisen Sopijapuolen tämän Tietoturvallisuusliitteen ehtojen vastaisesta toiminnasta, ellei kyse ole Pääsopimuksen mukaisesta ylivoimaisesta esteestä.

(2) Tämän Tietoturvallisuusliitteen mukaisen korvausvastuun enimmäismäärä on korvausvastuun ajankohtaa edeltävän kahdentoista kuukauden aikana Tilaajan Toimittajalle maksama sopimushinta. Sopijapuolet eivät vastaa välillisestä vahingosta.

(3) Jos rekisteröidylle aiheutuu vahinkoa tietosuojalainsäädännön rikkomisesta, kumpikin Sopijapuoli vastaa rekisteröidylle itse aiheuttamastaan vahingosta Tietosuoja-asetuksen 82 artiklan mukaisesti. Kumpikin Sopijapuoli vastaa itse Tietosuoja-asetuksen 83 artiklan mukaisista hallinnollisista sakoista.

15. Liitteet

Liite A – Details of Processing