

Turvallisuusliite

30.10.2018

Sisällys

1.	Tausta ja määritelmät	3
2.	Luottamuksellisuus ja salassapito	3
3.	Pääsy tiloihin.....	4
4.	Pääsy järjestelmiin ja tietoihin	5
5.	Turvallisuusselvitykset.....	5
6.	Tietoturvallisuus	6
7.	Rekisterinpito.....	7
8.	Alihankkijat.....	7
9.	Tarkastukset ja raportointi	8
10.	Korvaukset	9
11.	Turvallisuusliitteen voimassaolo.....	9

1. Tausta ja määritelmät

1.1 Tämä liite kuvaa turvallisuuteen, tietoturvaan ja tietosuojaan liittyvät sitoumukset ja toimintamallit. Tämä liite on olennainen osa Asiakkaan ja Toimittajan välistä sopimusta, jonka liitteenä tämä on (jäljempänä ”Sopimus”).

1.2 Sopijapuolet tiedostavat, että Sopimuksen perusteella toimitettaviin Palveluihin sisältyy sellaista tietoa, jonka salassa pysyminen on yhteiskunnan häiriöttömän toimintakyvyn ja kuntien sekä yksilöiden turvallisuuden kannalta kriittistä. Tällä Turvallisuusliitteellä sopijapuolet pyrkivät varmistamaan, että Salassa pidettävät tiedot pysyvät salassa.

1.3 Salassa pidettävä tieto tarkoittaa kaikkea sellaista Asiakkaan Toimittajalle luovuttamaa tai Toimittajalla olevaa Asiakkaan asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä ”julkisuuslaki”) tai muussa lainsäädännössä, ja jonka Asiakas on tällaiseksi tiedoksi merkinnyt tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin. Salassa pidettäväksi tiedoksi katsotaan myös julkisuuslaissa tarkoitetun ei vielä julkisen asiakirjan sisältämä tieto. Lisäksi kaikki Asiakkaan Toimittajalle luovuttamat henkilötiedot katsotaan Salassa pidettäväksi tiedoksi. Salassa pidettäväksi tiedoksi ei kuitenkaan katsota sellaista tietoa, joka on julkisesti saatavilla tai jonka sopijapuoli on saanut tietoonsa laillisella tavalla kolmannelta osapuolelta ilman sitä koskevaa salassapitovelvollisuutta. Julkisuuslaissa käytetty salassapidon käsite sisältää asiakirjasalaisuuden, vaihtolovelvollisuuden ja salassa pidettävien tietojen hyväksikäytökiellon.

1.4 Tilat tarkoittavat tässä Turvallisuusliitteessä sellaisia Toimittajan tai sen alihankkijan tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja.

2. Luottamuksellisuus ja salassapito

2.1 Tässä Turvallisuusliitteessä kuvattuja turvallisuusjärjestelyjä noudatetaan aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa.

2.2 Asiakas noudattaa julkisyhteisönä julkisuuslaissa sekä muussa lainsäädännössä olevia salassapitoa ja julkisuutta koskevia säännöksiä. Sopimuksella ei voida poiketa lainsäädännön Asiakkaalle asettamista pakottavista velvoitteista.

2.3 Toimittaja sitoutuu pitämään salassa kaikki Asiakkaan sille luovuttamat tai sillä olevat tai toimeksiannon toteuttamisessa syntyneet Salassa pidettävät tiedot, ottaen lisäksi huomioon kohdassa 2.7 sovitun. Salassa pidettäviä tietoja ei myöskään saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi.

2.4 Toimittajan tulee käsitellä 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.

2.5 Toimittaja sitoutuu säilyttämään ja käsittelemään Salassa pidettäviä tietoja siten, että ne pysyvät vain niiden henkilöiden hallussa, joilla on oikeus Salassa pidettäviin tietoihin, eivätkä ne joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

2.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille saattaa olla rikoslain mukaan rangaistava teko.

2.7 Tiedon antamisesta asiakirjasta, joka on saatu Asiakkaalta tai laadittu Asiakkaan toimeksiantotehtävää suoritettaessa, päättää Asiakas, jollei toimeksiannosta muuta johdu.

2.8 Toimittaja vastaa siitä, ettei Asiakkaan kohteiden tai toiminnan turvallisuus vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Sopimuksen vastaisen toiminnan johdosta.

2.9 Toimittaja ja sen alihankkijat saavat mainita referenssinä tehneensä työtä Asiakkaalle vain, jos asiasta on erikseen kirjallisesti sovittu.

2.10 Mikäli Toimittajalle syntyy tekijänoikeus tai muu immateriaalioikeus kaupallisen sopimuksen perusteella, ei se sisällä oikeutta julkistaa tämän liitteen perusteella salassa pidettävää tietoa.

3. Pääsy tiloihin

3.1 Toimittajan ja sen alihankkijan Tilojen tulee olla asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi Tiloihin ja siellä oleviin salassa pidettäviin tietoihin.

3.2 Mikäli Palvelu suoritetaan Toimittajan tai sen alihankkijan Tiloissa, Toimittajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. erityistilanteiden varalta. Asiakas ja Toimittaja sopivat tarvittaessa Palveluun liittyvistä tarkemmista vaatimuksista.

3.3 Henkilöt, joille ei ole myönnetty oikeutta Salassa pidettäviin tietoihin tai niitä sisältäviin järjestelmiin luvun 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.

3.4 Henkilöiden, joilla on pääsy Tiloihin, tulee olla tunnistettavissa.

4. Pääsy järjestelmiin ja tietoihin

4.1 Toimittaja vastaa siitä, että Salassa pidettäviä tietoja annetaan tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin, ja jotka ovat tietoisia salassapitoa koskevasta velvoitteistaan.

4.2 Toimittaja vastaa siitä, että Salassa pidettävien tietojen käsittelyyn osallistuvat Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt sekä henkilöt, joilla on pääsy Toimittajan järjestelmiin, joissa säilytetään Salassa pidettäviä tietoja, noudattavat tätä Sopimusta ja sen Turvallisuusliitettä.

4.3 Toimittaja vastaa siitä, että henkilö, joka käsittelee Salassa pidettäviä tietoja ja/tai jolla on pääsy järjestelmiin, joissa Salassa pidettäviä tietoja säilytetään, hyväksyy Asiakkaan hyväksymän salassapitositoumuksen ennen kuin hän aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin.

4.4 Palveluhenkilöstön käytön ja mahdollisen työskentelyn Asiakkaan tiloissa on aina oltava Asiakkaan turvallisuus-, tietosuoja-, yleisten käytös- sekä muiden Asiakkaan kohtuullisten ohjeiden ja määräysten mukaista. Asiakkaan on ilmoitettava etukäteen kaikista tällaisista Toimittajan henkilöstön noudatettaviksi tarkoitetuista menettelytapavelvoitteista.

5. Turvallisuusselvitykset

5.1 Jollei toisin sovita, jotta henkilö saa oikeuden käsitellä sellaisia Salassa pidettäviä tietoja, joiden salassapito on välttämätöntä turvallisuusselvityksissa (726/2014) mainittujen etujen suojaamiseksi, ja/tai päästä järjestelmiin, jotka sisältävät sellaisia Salassa pidettäviä tietoja, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettu turvallisuusselvitys, tai tarvittaessa tasoltaan vastaava ulkomainen turvallisuusselvitys. Toimittajan tulee hankkia turvallisuusselvityksen kohteena olevan henkilön suostumus selvityksen tekemiseen.

5.2 Jollei toisin sovita, tasoltaan vastaavaksi ulkomaiseksi turvallisuusselvitykseksi voidaan katsoa ainoastaan ulkomaisen kansallisen turvallisuusviranomaisen (esim. General Security Agreement:in eli GSA:n mukainen National Security Authority, NSA) tekemä turvallisuusselvitys (Personal Security Clearance, PSC).

5.3 Mikäli Toimittaja käyttää Palvelun toteutuksessa sellaista alihankkijaa, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee tästä alihankkijasta Toimittajan hakea yhteisöturvallisuusselvitys (Facility Security Clearance, FSC) ja tietojen käsittelyyn osallistuvista henkilöistä henkilöturvallisuusselvitys (Personal Security Clearance, PSC), jollei toisin sovita.

5.4 Jollei toisin sovita, Asiakkaan tehtävänä on hakea tässä luvussa, paitsi kohdassa 5.3, tarkoitettuja turvallisuus selvityksiä.

5.5 Asiakas vastaa kohdissa 5.1–5.2 tarkoitettujen turvallisuus selvitysten kustannuksista. Mikäli turvallisuus selvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai Toimittajan alihankkijan henkilöstössä tapahtuu vaihdos tai Asiakkaasta riippumaton lisäys, Toimittaja vastaa uuden henkilön turvallisuus selvityksen teettämisen kustannuksista.

5.6 Toimittajan tulee toimittaa turvallisuus selvityksen kohteena olevan henkilön täyttämä ja allekirjoittama turvallisuus selvityshakemuslomake Asiakkaalle turvallisuus selvityksen teettämistä varten. Lomakkeen tulee sisältää selvityksen kohteena olevan henkilön suostumus turvallisuus selvityksen tekemiseen. Jos turvallisuus selvitys tulee tehtäväksi sellaisessa valtiossa, jonka lainsäädännön mukaan kyseessä olevan selvityksen tekeminen ei edellytä selvityksen kohteena olevan henkilön suostumusta, Toimittajan ei myöskään tämän kohdan nojalla tarvitse pyytää henkilöltä edellä mainittua suostumusta.

6. Tietoturvaluisuus

6.1 Toimittaja noudattaa julkisuus laissa tarkoitettua hyvää tiedonhallintaa sekä EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 edellyttämää hyvää riskienhallintaa henkilötietojen käsittelyssä ja tietojen suojaamista koskevia säännöksiä sekä muuta tietosuoja koskevaa lainsäädäntöä Sopimukseen liittyvän Palvelun tuottamisessa.

6.2 Toimittaja valvoo ja pitää kirjaa hallinnoimistaan ja luovuttamistaan käyttövaltuuksista sekä niiden käytöstä.

6.3 Asiakkaan tietojärjestelmien ylläpidossa tulee käyttää henkilökohtaisia käyttäjätunnuksia, jotta eri toimenpiteiden suorittajat voidaan jälkikäteenkin yksilöidä. Yhteiskäyttötunnuksia voidaan käyttää vain poikkeustapauksissa, jos se on perustellusta syystä välttämätöntä ja siitä on kirjallisesti ilmoitettu asiakkaan sopimusyhteys henkilöille tai erikseen sovitulle tietoturvaluisuusasioiden yhteys henkilöille.

6.4 Toimittajan on ylläpidettävä ajantasaista tietoa sellaisista Palvelun tuottamiseen osallistuvista Toimittajan tai sen alihankkijan henkilöistä, joilla on pääsy Asiakkaan kanssa määriteltyihin Asiakkaan tietoaineistoihin ja tunnistetietoihin. Toimittajan on annettava listaus edellä mainituista henkilöistä Asiakkaan nähtäväksi Asiakkaan pyynnöstä. Toimittajan on myötävaikutettava siihen, että Asiakas voi tarvittaessa teettää turvallisuus selvitykset edellä mainituista henkilöistä.

6.5 Toimittaja on tietoinen ja hyväksyy sen, että tietojärjestelmien keräämiä käyttölokiteitoja voidaan käyttää käytön valvontaan, virhetilanteiden, tietomurtojen tai muiden väärinkäytösten ja niiden yritysten selvittämiseen.

6.6 Tietojen väärinkäyttötilanteissa tai vahvoissa epäilyissä Asiakkaalla on oikeus välittömästi poistaa tai vaatia poistettavaksi väärinkäyttöksiin syyllistyneen käyttöoikeudet Palveluun liittyvistä tietojärjestelmistä.

6.7 Kaikki Palvelun tuottamisessa syntyvä tietosuojattava jäte pitää hävittää asianmukaisesti.

6.8 Mikäli Toimittaja tuottaa laitteiden kierrätys ja romutuspalvelua, Toimittaja vastaa laitteiden kierrätyksen yhteydessä siitä, etteivät laitteissa olevat tiedot päädy sivullisille.

7. Rekisterinpito

7.1 Asiakas toimii rekisterinpitäjänä palveluntuottamisessa käytettävien henkilörekisterien osalta omassa organisaatiossaan määriteltyjen dokumenttien mukaisesti.

7.2 Palveluntuottamisessa käsitellään henkilörekistereitä, joita Toimittaja käsittelee Asiakkaan lukuun eli Toimittaja toimii Henkilötietojen käsittelijäorganisaationa. Toimittaja säilyttää kyseisiin rekistereihin sisältyviä tietoja huolellisesti ja hyvän tietojenkäsittelytavan mukaisesti ja siten, että tiedot säilyvät virheettöminä ja eheinä. Tiedot pitää säilyttää teknisesti omassa loogisessa kokonaisuudessaan siten, että ne ovat eroteltavissa selkeästi erilleen Toimittajan omista rekisteritiedoista.

7.3 Toimittajalla ei ole oikeutta käyttää Asiakkaan rekistereitä omassa toiminnassaan ilman Asiakkaan lupaa.

7.4 Toimittaja sitoutuu noudattamaan rekistereihin sisältyvien tietojen käsittelyssä Suomessa voimassaolevia säädöksiä sekä Asiakkaiden ohjeita ja määräyksiä ja vastaa siitä, että niitä käsittelevät ja niihin pääsevät vain henkilöt, joiden työtehtävien kannalta se on välttämätöntä. Jälkikäteen pitää pystyä yksilöimään tarkasti kuka on käsitellyt salassa pidettäviä rekisteritietoja ja milloin.

7.5 Toimittaja sitoutuu antamaan pyydettyä Asiakkaalle selvityksen rekistereihin liittyvien tietojen käsittelystä ja säilyttämisestä.

7.6 Henkilötietojen käsittelyn velvoitteista ja vastuista sovitaan erillisellä liitteellä Henkilötietojen käsittelyn ehdot (liite 2.1)

8. Alihankkijat

8.1 Toimittajan tulee hyväksyttäväksi Asiakkaalla sellainen alihankkija, jota se aikoo käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Tiloihin. Tässä Turvallisuusliitteessä alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Tiloihin.

8.2 Mitä tässä Sopimuksessa on sovittu Toimittajan henkilöstöstä, sovelletaan myös Alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.

8.3 Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tätä Turvallisuusliitettä myös käyttäessään alihankkijoita. Toimittajan on tiedotettava alihankkijalleen, että turvallisuusjärjestelyjen saattamisesta tämän Turvallisuusliitteen edellyttämälle tasolle saattaa syntyä kustannuksia. Asiakas ei vastaa näistä kustannuksista.

8.4 Toimittaja vastaa siitä, että sen alihankkijat toimivat tämän Turvallisuusliitteen sekä Henkilötietojen käsittelyn ehdot -liitteen ehtojen mukaisesti.

9. Tarkastukset ja raportointi

9.1 Asiakkaalla tai Asiakkaan määräämällä kolmannella taholla (joka ei ole Toimittajan suoranainen kilpailija) on oikeus tarkastaa etukäteen ilmoitettu ajankohtana Toimittajan ja sen alihankkijoiden tietoturvaan, tietosuojaan ja turvallisuuteen liittyvät menettelyt tätä Turvallisuusliitettä sekä Sopimusta koskevilta osin. Tarkastuksen suorista kustannuksista vastaa Asiakas, mikäli muuta ei sovita. Välillisiä kustannuksia ei korvata. Asiakkaan on ilmoitettava tahdostaan suorittaa tarkastus viimeistään 3 viikkoa (21 päivää) ennen ehdotettua tarkastuspäivää. Toimittaja voi ehdottaa uutta päivää tarkastukselle. Uusi ajankohta ei kuitenkaan saa olla myöhemmin kuin kymmenen (10) päivää Asiakkaan ehdottaman päivän jälkeen. Tarkastus saadaan suorittaa kuitenkin enintään kaksi kertaa vuodessa, ellei ole erityisen painavia syitä useammille tarkastuksille. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainituista määrärajoista riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tietoturvasuutta tai Toimittajan tai sen alihankkijoiden salassapitovelvoitteita muita asiakkaita kohtaan

9.2 Toimittajan tulee huolehtia sopimusjärjestelyin siitä, että Asiakkaalla on mahdollisuus tarkastaa myös Toimittajan sellaisen alihankkijan turvallisuusjärjestelyt, joka osallistuu Salassa pidettävien tietojen käsittelyyn.

9.3 Mikäli tarkastuksessa havaitaan merkittäviä puutteita turvallisuusjärjestelyissä, Toimittaja korvaa Asiakkaalle tarkastuksesta aiheutuneet kustannukset.

9.4 Toimittajan tulee korjata tarkastuksessa havaitut puutteet viivytyksettä, kuitenkin viimeistään 30 vuorokauden kuluessa Asiakkaan kirjallisesta ilmoituksesta, ellei siitä ole Asiakkaan ja Toimittajan välillä erikseen toisin sovittu. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvalisuudelle, on korjattava heti. Asiakas ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.

9.5 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, jos Toimittajan tai sen alihankkijan tämän Turvallisuusliitteen kannalta keskeisissä toiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai jos Toimittajan tai sen alihankkijan omistussuhteissa tapahtuu merkittäviä muutoksia.

9.6 Toimittaja valvoo tämän Turvallisuusliitteen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Asiakkaalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Asiakas seuraa Palvelun turvallisuustason toteutumista yhteistyössä Toimittajan kanssa.

9.7 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, mikäli Toimittajaan kohdistuu Asiakasta mahdollisesti uhkaavia yhteydenottoja

9.8 Toimittaja on velvollinen raportoimaan välittömästi Asiakkaan sopimusyhteyshenkilölle tai erikseen sovitulle tietoturvallisuusasioiden yhteyshenkilölle Sopimuksen alaisen toiminnan piiriin kuuluvasta tietovuodosta, tietoturvahkasta tai muusta turvallisuutta vaarantavasta tapahtumasta.

9.9 Asiakkaalla ei ole täyttä kontrollia palvelun tuotantoprosessista ja siihen liittyvistä tiedoista. Kuitenkin palveluntuotantoprosessin riskit ja niiden hallinnan taso vaikuttavat Palvelun käyttäjiin. Asiakkaalla on tarve saada riittävä varmuus ulkoistettujen palveluiden valvonnan asianmukaisuudesta. Tämän vuoksi Toimittajan tulee veloituksetta toimittaa Asiakkaalle vuosittain raportti siitä, miten Toimittaja hallitsee ja reagoi sekä toimintaansa että Palveluun liittyviin riskeihin. Toivottavaa on, että raportti teetetään luotettavalla riippumattomalla ulkoisella osapuolella.

10. Korvaukset

10.1 Asiakkaalla on oikeus saada korvaus kaikista niistä välittömistä vahingoista sekä kuluista ja kustannuksista, jotka sille ovat aiheutuneet Toimittajan tähän Turvallisuusliitteeseen kohdistuvasta sopimusrikkomuksesta, ellei rikkomus ole aiheutunut Liitteessä 6 (Asiakkaan vaatimukset valmiussuunnitelmasta) tarkoitetusta ylivoimaisesta esteestä.

10.2 Lisäksi Asiakkaalla on oikeus saada korvaus myös kaikista välillisistä vahingoista, mikäli vahinko on aiheutettu salassapitovelvollisuutta rikkoen.

11. Turvallisuusliitteen voimassaolo

11.1 Tämä liite on voimassa niin kauan kuin Sopimus on voimassa, Toimittajalla on Asiakkaan salassa pidettäviä tietoja hallussaan tai Asiakas tosiasiallisesti käyttää Toimittajan Sopimuksen mukaisia Palveluita tai tuotteita. Tässä kuvatut salassapitovelvollisuutta koskevat kohdat ovat voimassa myös Sopimuksen voimassaolon päätyttyä tai Sopimuksen irtisanomisen tai purkamisen jälkeen.

11.2 Pääsopimuksen päätyttyä Toimittaja mahdollisine alihankkijoineen palauttaa kaikki Asiakkaan Salassa pidettäviä tietoja sisältävät dokumentit, tallenteet ja muun materiaalin. Erikseen kirjallisesti niin sovittaessa Toimittaja mahdollisine alihankkijoineen voi myös tuhota edellä mainitun materiaalin. Aineistoa ei saa hävittää, mikäli laki tai viranomaisten määräykset vaativat sen säilyttämistä.