KEUSOTE
Keski-Uudenmaan hyvinvointialue

Tietoturvaliite

Pääsopimuksen liite 2

Sote ihmisen kokoiseksi.

1.1.2023

Sisällysluettelo

1. Yleiset ehdot

Sopijapuolten välisessä sopimuksessa sovittujen palvelujen häiriöttömyys ja luotettavuus sekä Asiakkaan toiminnan jatkuvuus sekä asiakastiedon tietoturva ja tietosuoja ovat erittäin tärkeitä. Sopijapuolet toteavat, että palveluiden luotettavuutta voidaan kehittää turvallisuuden hallinnan avulla ja korostavat yhteistyön merkitystä turvallisuuden ja tietoturvan hallinnassa. Näistä syistä sopijapuolet sopivat tässä kohdassa turvallisuutta ja tietoturvallisuuden hallintaa koskevista vastuista ja velvollisuuksista.

Toimittajan tulee huolehtia käsittelemiensä tietojen asianmukaisesta suojaamisesta laittoman tai tapaturmaisen häviämisen tai hävittämisen varalta. Toimittajalla on sopimuksen voimassaoloajan velvollisuus säännöllisesti raportoida, sekä Asiakkaan niin erikseen pyytäessä esittää yksityiskohtaisempi selvitys siitä, miten Toimittaja varmistaa turvallisuus- ja tietoturvavaatimusten täyttymisen.

Näiden lisäksi, tai näihin sisältyen, tuotetun palvelun tulee toteuttaa myös seuraavat vaatimukset:

2. Tietoturvapolitiikka, hallinta ja arviointi

Asiakkaalle tai sen osoittamalle kolmannelle auditoivalle osapuolelle (joka yhdessä Toimittajan kanssa etukäteen sovitaan) tulee tarjota mahdollisuus:

- nähdä tai saada selvitys Toimittajan tietoturvapolitiikasta palveluun liittyviltä osin
- nähdä tai saada selvitys Toimittajan tietoturvaohjeistuksesta palveluun liittyviltä osin
- saada auditoinnin tuloksista raportti niiden palveluiden osalta, joita Asiakas käyttää
- tehdä palvelua tai sen osaa koskevia tietoturva-auditointeja

Alihankkijoihin ja heidän osuuteensa Palveluista sovelletaan samoja vaatimuksia, kuin Toimittajaan itseensä.

3. Turvallisuuden ja tietoturvallisuuden johtaminen

Toimittajan vastuulla on tunnistaa ydintoimintoihinsa liittyvät jatkuvuuden, erityistilanteiden hallintaa ja tietoturvallisuutta uhkaavat ja ohjaavat tekijät ja velvoitteet, kuten keskeinen lainsäädäntö, sekä ydinprosessiensa vaatimukset ja riskit. Turvallisuuden, riskienhallinnan ja jatkuvuuden turvaamisen tulee olla osa Toimittajan johtamista sekä sopimuksen kohteena olevien palvelujen suunnittelua ja toteutusta.

Sopijapuolet pyrkivät osaltaan estämään Asiakkaan toiminnalle tärkeiden tietojen ja tietojärjestelmien valtuudettoman tai asiattoman käytön sekä ennalta ehkäisemään ja rajaamaan häiriöistä ja rikkomuksista aiheutuvia vahinkoja. Asiakkaan vastuulla on määritellä ja priorisoida toiminnalleen kriittiset ja tärkeät tiedot ja tietojärjestelmät.

Toimittajan tulee pystyä pyynnöstä todentamaan Asiakkaalle, että se käsittelee sekä Asiakkaan liiketoiminnalle että Toimittajan omalle toiminnalle tärkeiksi tai kriittisiksi luokiteltuja tietoja luokittelu- ja käsittelyohjeiden mukaisesti koko tiedon elinkaaren ajan. Toimittaja ja Asiakas käyvät yhdessä läpi tietojen toistensa tietojen luokittelu- ja käsittelyohjeet ja sopivat yhteiset menettelytavat Sopimuksen voimassaoloaikana.

Toimittaja kuvaa, ohjeistaa ja vastuuttaa palvelun häiriötilanteisiin liittyvän oman päätöksentekoprosessinsa ja tietoturvapoikkeamien käsittelyn. Toimittajalla tulee olla dokumentoitu ja henkilöstölle koulutettu tapa toimia turvallisuus- poikkeamissa ja väärinkäytöstilanteissa. Dokumentoinnista tulee käydä ilmi, kenelle poikkeamat raportoidaan sekä poikkeamien vakavuus- ja seurausasteet.

4. Tietojärjestelmien yleiset turvallisuusvaatimukset

Järjestelmädokumentointi vaaditaan kaikista uuden järjestelmän komponenteista. Tämä sisältää tarkat kuvaukset myös järjestelmien välisistä yhteyksistä ja protokollista. Järjestelmän muuttuessa oleellinen osa muutosta on järjestelmädokumentaation päivitys.

Uusia käyttöjärjestelmiä, tietokantoja, sovelluspalvelimia jne. ei saa asentaa oletusturvallisuusasetuksin, vaan ne pitää ns. koventaa (hardening). Koventamisessa tulee käyttää jotakin alan hyvää käytäntöä kuten esimerkiksi CIS Benchmarkien mukaiset kovennukset eri palveluille ja käyttöjärjestelmille (https://www.cisecurity.org/cybersecurity-best-practices/). Kriittiset järjestelmätiedostot pitää tunnistaa ja suojata asianmukaisin käyttöoikeuksin. Ne pitää suojata erityisesti asiattomilta muutoksilta.

Käyttö- ja tietojärjestelmissä on virheitä, jotka aikaansaavat turvallisuusaukkoja, joita julkistetaan ja joita myös hyväksikäytetään. Siten kaikkien järjestelmien osalta Toimittajan on aktiivisesti seurattava turvallisuusaukkojen kehitystä ja poistettava ne asianmukaisesti.

Toimittajan on seurattava ja reagoitava etenkin Suomen CERT'in sekä ohjelmisto- ja laitetoimittajien varoituksiin ja hälytyksiin.

Käyttö- ja varusohjelmistojen päivitysten osalta Toimittajan on laadittava hallintasuunnitelma, jossa on huomioitava sekä kriittisten päivitystarpeiden, että kiireettömämpien päivitysten hoito.

Toimittaja seuraa myös muiden palveluunsa kuuluvien ohjelmistojen osalta niitä koskevia tietoturvallisuusvaroituksia ja tekee tarvittavat korjaukset mahdollisimman pian. Korjausmenettelyt on suunniteltava ja huomioitava jo ohjelmistojen käyttöönoton yhteydessä.

5. Sovelluskehitys

Mikäli sopimukseen kuuluu sovelluskehitystä, näiden osalta toimitaan seuraavasti: Sopijapuolet toteavat, että sovelluskehityksen ja ylläpidon tietoturvallisuus on Asiakkaalle hyvin tärkeää. Toimittaja soveltaa Asiakkaalle tehtävässä sovelluskehityksessä turvallisen sovelluskehityksen käsikirjaa (https://www.suomidigi.fi/sites/default/files/2020-05/Turvallisen%20sovelluskehityksen%20k%C3%A4sikirja.pdf) tai muuta kirjallista sovelluskehityksen tietoturvallisuuden varmistamaa mallia.

6. Päätelaite- ja palvelinturvallisuus

Toimittaja huolehtii kaikkien palveluun liittyvien pääte- ja palvelinlaitteistojensa tietoturvallisuudesta sekä ajanmukaisesta haittaohjelmistojen torjunnasta.

Tietojärjestelmissä (palvelimilla) oleva tieto varmistetaan siten, että se voidaan tarvittaessa palauttaa toisiin tietokoneisiin alkuperäisen kaltaisesti toimivaksi kokonaisuudeksi.

7. Tietoverkon hallinta ja käytön turvallisuus

Toimittaja eriyttää omat tietoverkkonsa teknisesti siten, että eri ympäristöt ja järjestelmät, esim. tietokannat ja sovelluspalvelimet, ovat kukin omissa verkoissaan.

Toimittajan palvelussa käyttämien etäyhteyksien pitää olla salattuja, esim. VPN-yhteyksiä. Käytössä pitää olla käyttäjän vahva tunnistus.

Toimittajan Asiakkaalle tarjoamassa palvelussa sisäinen ja ulkoinen tietoliikenne tulee hoitaa turvallisesti siten, että luvattomat sisään kirjoittautumisyritykset voidaan tunnistaa ja automaattisesti estää.

8. Käyttövaltuuksien hallinta

Toimittajan käyttämää käyttövaltuushallintaa koskevat seuraavat ehdot:

Toimittajan palveluun käyttämät tunnukset ja käyttövaltuudet tulee olla keskitetyssä käyttövaltuushallinnassa.

Järjestelmiin pitää määrittää roolit eri tehtäville siten, että pääsy järjestelmiin perustuu pääsääntöisesti jäsenyyteen rooliin liittyvässä ryhmässä. Roolimäärittelyn pitää olla niin tarkalla tasolla, että vaarallisten työyhdistelmien syntyminen estyy (segregation of duties). Pääsyn järjestelmiin pitää perustua työtehtävään.

Järjestelmätunnuksille pitää määritellä myös tarvittavat roolit ja pääsyoikeudet. Myös järjestelmätunnuksilla tehdyt operaatiot pitää olla jäljitettävissä yksittäiseen henkilöön. Järjestelmätunnusten käyttö järjestelmittäin määritellään yhteisesti käynnistysprojektin osana.

9. Päivitykset ja muutoshallinta

Toimittajan päivitys- ja muutoksenhallintatoimintamalleja koskevat seuraavat ehdot:

Käytössä pitää olla kaikkia järjestelmäkomponentteja koskeva muodollinen muutoksenhallintaprosessi asianmukaisine lupakäytäntöineen. Muutoksenhallintaprosessin vastuut pitää olla selkeästi kuvattu.

Haavoittuvuuksienkäsittelyprosessin pitää olla dokumentoitu ja sen pitää sisältää kuvaukset monitorointi- ja päivitystavoista sekä vastuista.

10. Audit Trail

Toimittajan palvelujen audit trail:

Järjestelmien lokitiedoista pitää selvitä kuka teki, mitä ja milloin. Tietojärjestelmien kaikkia tasoja (käyttöjärjestelmä, tietokanta, sovellus jne.) pitää lokittaa. Lokitiedot pitää suojata siten, että niitä ei päästä muuttamaan. Lokitietoihin liittyvät käsittelytoimet tulee myös lokittaa. Lokitietoja pitää säilyttää vähintään puoli vuotta, ellei sopimuksellisesti ole toisin sovittu. Lokitietojen mahdollinen kopiointi Asiakkaan hallussa olevaan toiseen järjestelmään sovitaan erikseen.

11. Henkilöstöturvallisuus

Toimittajan tulee tehdä selvitys siitä, miten varmistetaan henkilöstön luotettavuus, erityisesti niissä tilanteissa, joissa henkilöstöllä on pääsy Asiakkaan salassa pidettäviin, arkaluonteisiin tai luottamuksellisiin tietoihin, ja myös siitä, miten henkilöstön tietoturvaosaaminen pidetään yllä.

Toimittaja nimeää Asiakkaalle palvelua toteuttavat henkilöt (ne, joilla on pääsy Asiakkaan aineistoihin tai järjestelmiin ja nimetyt avainhenkilöt) ja heiltä voidaan vaatia suostumusta turvallisuusselvitykseen. Kaikista Asiakkaalle nimetyistä palvelua tuottavista henkilöistä tulee pystyä tekemään suomalainen perusmuotoinen turvallisuusselvitys tai vastaava ulkomainen turvallisuusselvitys. Asiakas tekee tietoturvakäytäntöjensä mukaisesti tarvittavista henkilöistä turvallisuusselvityksen ennen heidän pääsyään Asiakkaan palvelujen toteuttajiksi. Asiakas vastaa turvallisuusselvityksen suorista, kolmansille

osapuolille suoritettavista maksuista. Asiakkaalla on oikeus hyväksyä tai hylätä tarjoajan esittämä asiantuntija turvapolitiikkansa puitteissa.

Toimittaja perehdyttää ja kouluttaa säännöllisesti keskeiset palvelun turvallisuuteen ja tietoturvaan liittyvät vaatimukset, menettelytavat ja niiden muutokset omalle henkilöstölleen ja mahdollisille alihankkijoilleen henkilön työtehtävien mukaisesti.

Palvelun tuottamiseen osallistuva Toimittajan henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapauksista tai niiden uhkista tulee ilmoittaa ja miten ilmoitus tulee tehdä.

Asiakkaalla on oikeus vaatia turvallisuusselvitysten tekemistä koskien palvelun tuottajan henkilöstöä, jotka käsittelevät Asiakkaan järjestelmiä tai tietoja.

12. Fyysinen turvallisuus ja konesalit

Kulkuoikeudet toimittajan hyödyntämiin laitetiloihin on rajoitettu vain nimetylle käyttö- ja huoltohenkilöstölle ja laitetilat pidetään aina lukittuina.

Toimittajan Asiakkaalle tarjottavien palveluun liittyvien tilojen turvallisuuden varmistamisen periaatteista ja mahdollisista sertifioinneista saadaan sopimuksen kohteena olevien palvelujen näkökulmasta riittävä selvitys pyydettäessä.

13. Jatkuvuuden hallinta

Toimittajan palvelujen jatkuvuuden hallinnan tulee täyttää kulloisetkin sopimuksessa kuvatut jatkuvuusvaatimukset.

13.1 Strateginen ohjaus

Toimittaja on tunnistanut palvelun tuottamiseen liittyvät jatkuvuuden ja erityistilanteiden hallintaa sekä tiedon turvaamista ohjaavat tekijät, velvoitteet ja riippuvuudet.

Toimittaja käy yhdessä Asiakkaan kanssa läpi sen tuottamien palveluiden merkityksen varautumisvelvollisen Asiakkaan liiketoiminnalle ja suunnittelee palvelujen varautumis- ja jatkuvuusvaatimuksia ottaen huomioon Asiakkaan palvelujen jatkuvuuden.

Toimittajalla on menettely palveluihin liittyvien ulkoisten vaatimusten tunnistamiseksi ja näiden tarpeiden ja muutosten viemiseksi toiminnan suunnitteluun.

13.2 Organisointi ja resursointi

Toimittajalla jatkuvuuden hallinta ja Asiakkaiden tiedon turvaaminen on organisoitu ja vastuutettu osana palvelun normaalia toimintaa sekä kumppanuusverkoston hallintaa.

Toimittaja määrittelee erityistilanteiden hallinnan ja poikkeusolojen toiminnan roolit ja vastuut omassa organisaatiossaan sekä alihankkijaverkostossaan ja resursoi nämä tehtävät sovittujen palvelujen edellyttämässä laajuudessa.

Toimittaja tunnistaa palveluihin liittyvät toimintaympäristöt ja niihin liittyvät Asiakkaan keskeiset toiminnot. Asiakas kuvaa kyseisten toimintojen kriittisyyden omalle toiminnalleen. Toimittaja ottaa systemaattisesti palvelujen jatkuvuussuunnittelussaan huomioon Asiakkaan kuvaaman kriittisyyden.

Toimittaja suunnittelee ja sopii palvelujen jatkuvuuden hallinnan omassa toimintaverkostossaan.

Toimittaja laatii hankittavan palvelun kannalta kriittisille palveluille yksityiskohtaiset kohdekohtaiset ohjeet ja kouluttaa ne avainhenkilöille keskeisimpien häiriötilanteiden varalta.

13.3 Kumppanuudet

Toimittaja varmistaa palvelun jatkuvuuden edellyttämien verkoston palvelujen ja muiden resurssien käytettävyyden häiriö- ja erityistilanteissa.

Toimittajalla on menettely, jolla se varmistaa, että sen palveluun liittyvät alihankkijat ja toimittajaverkosto pystyvät vastaamaan palvelun edellyttämiin jatkuvuus- ja varautumisvaatimuksiin. Toimittaja pystyy näyttämään toteen tämän menettelyn.

13.4 Palvelujen varmistaminen erityistilanteissa

Toimittaja sopii alihankkijaverkostossaan vastuut resurssien hallinnasta ja saatavuudesta. Toimittaja varmistaa keskeisen alihankkijaverkostonsa kyvyn tuottaa palvelun kannalta keskeisiä palveluja häiriötilanteissa.

13.5 Palveluihin liittyvät toimittajan ICT- ratkaisut

Palvelun tuottamisessa ja suunnittelussa otetaan huomioon jatkuvuuden hallintaan, tiedon turvaamiseen ja varautumiseen vaikuttavat keskeiset tekijät. Toimittaja on varmistanut Palvelun liittyvän palvelutuotantonsa ja hallinnan prosessit ja niillä on varamenettelyt.

Toimittaja suunnittelee, sopii, ohjeistaa ja kouluttaa tuotantomuutokset ja varajärjestelyihin siirtymisen ja toipumisen prosessit häiriö- ja erityistilanteissa.

Palveluun liittyvät kriittisten toimintojen vaatimat tietoaineistot on turvattu häiriö- ja erityistilanteissa.

Tässä liitteessä esitetyt vaatimukset koskevat myös esim. virtuaaliympäristöjä ja varmistusjärjestelmiä.

13.6 Jatkuvuustestaukset
Toimittaja suunnittelee, tarvittaessa yhdessä Asiakkaan kanssa, Asiakkaan määrittämien keskeisten kriittistä tietoa sisältävien järjestelmien jatkuvuustestaukset tai muun ratkaisujen ja palvelujen jatkuvuutta varmistavan toimintamallin.

14. Erityistilanteiden hallinta

Toimittajan palveluun liittyvä erityistilanteiden hallinta on organisoitu, ohjeistettu ja huomioitu toimittajan toimintamalleissa.

Toimittaja määrittelee häiriötilanteen kriisiviestinnän periaatteet, vastuut ja menetelmät sekä mahdolliset varmentavat viestintävälineet sekä –menetelmät.

Viestinnän tulee kriisinkin aikana tapahtua salassapitoehtojen puitteissa.

15. Salassapito

Sopijapuolet huolehtivat omilla vastuualueillaan, että tiedon julkisuutta ja salassapitoa koskevat säädökset ja viranomaisten antamat määräykset otetaan huomioon.

Sopijapuolet voivat palvelujen tuottamisen yhteydessä luovuttaa ja ilmaista toiselle Sopijapuolelle liiketoimintaansa liittyviä teknisiä ja/tai kaupallisia tietoja ja muita aineistoja kirjallisessa, suullisessa ja/tai muussa muodossa (jäljempänä "Luottamukselliset tiedot"). Luottamukselliset tiedot voivat käsittää muun muassa turvaluokiteltua (salainen, luottamuksellinen tai sisäinen), taloudellista, teknistä, kaupallista, asiakas- tai muuta henkilötietoa, operatiivista ja/tai henkilöstöhallintoon liittyvää tietoa sekä muuta sopijapuolen tai sen nykyiseen tai tulevaan liiketoimintaan liittyvää tietoa liittyen esimerkiksi sopijapuolen tuotteisiin, talouteen, järjestelmiin, toimintamalleihin, teknisiin ja muihin prosesseihin, keksintöihin, ideoihin, suunnitelmiin ja/tai tietotaitoon.

Luottamuksellisia tietoja vastaanottava sopijapuoli sitoutuu seuraaviin salassapitovelvoitteisiin:

1. Vastaanottava sopijapuoli sitoutuu pitämään kaikki luovuttavalta sopijapuolelta vastaanottamansa Luottamukselliset tiedot salassa ja olemaan luovuttamatta tai ilmaisematta niitä edelleen kolmannelle osapuolelle (alihankkijat, tytäryhtiöt, jne.) ilman luovuttavan sopijapuolen etukäteen antamaa kirjallista suostumusta.
2. Vastaanottava sopijapuoli sitoutuu olemaan käyttämättä vastaanottamiaan Luottamuksellisia tietoja muuhun kuin yksinomaan sopimuksessa määriteltyjen velvoitteiden täyttämiseksi. Sovittua laajempi ja muuhun tarkoitukseen liittyvä luottamuksellisten tietojen käyttö edellyttää aina luovuttavan sopijapuolen etukäteen antamaa kirjallista suostumusta.
3. Vastaanottava sopijapuoli sitoutuu ilmaisemaan tai luovuttamaan luottamuksellisia tietoja vain sellaisille edustajilleen ja työntekijöilleen, joiden on välttämätöntä saada niistä tieto tarkoituksen toteuttamista varten. Vastaanottava sopijapuoli vastaa työntekijöidensä salassapitovelvoitteen noudattamisesta kuin omastaan. Vastaanottava sopijapuoli vastaa siitä, että vastaanottava sopijapuolen työntekijät ovat aina vähintään samantasoisen salassapitovelvoitteen sitomia kuin tässä sopimuksessa on sovittu.
4. Vastaanottava sopijapuoli sitoutuu säilyttämään vastaanottamansa luottamukselliset tiedot aina vähintään samalla huolellisuudella kuin vastaanottava sopijapuoli säilyttää omat luottamukselliset tietonsa.

Edellisten lisäksi Toimittaja sitoutuu vastaamaan siitä, että kaikki sen edustajat ja työntekijät noudattavat kulloinkin soveltuvia Asiakkaan turvallisuusohjeistuksen määräyksiä (kuten tietoturva- ja laatuvaatimuksia) palvelujen tuottamisen edellyttämässä laajuudessa, edellyttäen että Asiakas on antanut riittävät tiedot Asiakkaan turvallisuusohjeiden määräyksistä.

Palveluun tallennettu tai siinä käsiteltävä tieto on luottamuksellista ja Asiakkaan tai sen tytäryhtiön tai kolmannen osapuolen omistuksessa. Asiakkaan tai sen tytäryhtiön tai kolmannen osapuolen tietojen muokkaaminen, siirtäminen tai muu käsittely Toimittajan, alihankkijan tai automatisoituna ohjelmiston toimesta, ei vaikuta tietojen omistajuuteen tai käyttöoikeuksiin.

Toimittaja käsittelee Asiakkaan hallussa olevia henkilötietoja ja Asiakkaan muita tietoja sekä tietoja, joihin Toimittajalla on pääsy sen vuoksi, että Toimittaja on solminut sopimuksen Asiakkaan kanssa, yksinomaan välittömästi sopimuksessa määriteltyjen sopimusvelvoitteiden täyttämiseksi. Salassapitovelvollisuus ei koske luottamuksellisia tietoja, jotka

a) olivat yleisesti tiedossa luottamuksellisten tietojen luovutushetkellä tai tulevat myöhemmin yleiseen tietoon ilman, että vastaanottava sopijapuoli olisi menetellyt tämän sopimuksen vastaisesti, tai

b) olivat todistettavasti vastaanottavan sopijapuolen tiedossa tai hallinnassa jo ennen luottamuksellisten tietojen vastaanottamista luovuttavalta sopijapuolelta, tai
c) vastaanottava sopijapuoli on todistettavasti saanut kolmannelta osapuolelta ilman salassapitovelvollisuutta, tai
d) on todistettavasti itsenäisesti luonut vastaanottavan sopijapuolen henkilökunta, joka ei ole hyväksikäyttänyt luottamuksellisia tietoja.

Salassapitoehtojen rikkomuksista määräytyvä sopimussakko on kuvattu pääsopimuksessa.

Sopijapuolella on oikeus vaatia perustellusta syystä erillisen henkilökohtaisen salassapitositoumuksen allekirjoittamista niiltä toisen sopijapuolen tai tämän alihankkijan palveluksessa olevilta, jotka sopimuksen toteuttavat.

Salassapitoa koskevat ehdot ovat voimassa myös sopimuksen päättymisen jälkeen viisi (5) vuotta kunkin luottamuksellisen tiedon vastaanottamisesta. Asiakkaan salassa pidettävien ja arkaluonteisten tietojen osalta salassapitovelvollisuus on voimassa pysyvästi. Jos sopimus tai toimeksianto päättyy tai purkautuu, sopijapuoli palauttaa tai toisen sopijapuolen suostumuksella hävittää toisen sopijapuolen luottamuksellisen aineiston.

Sopimuksen päätyttyä tai purkauduttua kumpikin sopijapuoli ja näille suoritteita tehneet alihankkijat palauttavat kaikki työhön liittyvät toista sopijapuolta koskevat dokumentit ja muut tallenteet toisen sopijapuolen hallintaan viivyttelemättä.

Sopijapuolen tulee tuhota ne toisen sopijapuolen aineistot ja tallenteet tietoturvallisesti, joita ei sovita palautettavaksi, yhteisesti sovitulla tavalla 14 vuorokauden kuluessa sopimuksen päättymisestä, ellei toisin erikseen kirjallisesti sovita, huomioiden viranomaismääräykset ja pääsopimuksen toimittajan myötävaikutus sopimuksen päättyessä –kohdan ehdot.

Sopijapuolella on oikeus käyttää palvelun toimituksen yhteydessä hankkimaansa ammattitaitoa ja kokemusta.

15.1 Salassapitovelvoitteiden ulottuvuus

Toimittajan tulee saattaa Asiakkaan ja Toimittajan väliseen palvelun toimittamiseen liittyvä henkilöstönsä sekä mahdollisen alihankkijan henkilöstö tietoiseksi tämän liitteen salassapitovelvoitteista. Toimittaja vastaa siitä, että myös sen alihankkijat noudattavat tämän liitteen ehtoja.