Tietoturvallisuusliite

Tietoturvallisuusliite

[pp.kk.vvvv]

Vaasan kaupunki

ja

[Palveluntuottaja]

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

VAASA.

Dokumentin tiedot

Dokumentin nimi	Turvallisuusliite
Käyttötarkoitus	ICT-hankintojen sopimusliite tietoturvan ja tietosuojan osalta
Versio	1.0
Tila	Hyväksytty
Laatija	Sami Varjo
Tarkastaja	Timo Grev
Hyväksyjä	Teemu Lehtonen
Tiedon luokittelu	Julkinen asiakirja

Versionhallinta

Versio	Pvm	Laatija	Muutoksen lyhyt kuvaus
0.1	07.08.2020	Sami Varjo	Ensimmäinen luonnos muokkaukseen
0.2.	12.08.2020	Sami Varjo	Lisätty numerointi ja sisällysluettelo
0.3	14.08.2020	Sami Varjo	Päivitetty tietosuoja-kappaletta.
0.4	13.11.2020	Sami Varjo	Päivtetty kaupungin viralliselle dokumenttipohjalle ja lisätty sisällysluettelo.
0.5	23.11.2020	Timo Grev, Teemu Lehtonen	Katselmointi ja kommentointi
1.0	26.11.2020	Teemu Lehtonen	Dokumentti hyväksytty versioon 1.0

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

VAASA.

Sisällysluettelo

OHJE

Päivitä sivulla 4 sopimustiedot, poista tämä OHJE-kappale ja liitä tämä dokumentti sopimuksen liitteeksi.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

VAASA.

1. JOHDANTO

1.1. Tämä dokumentti on osapuolten välisen sopimuksen liite, jolla määritetään sopimuksen kohteen tietosuojaan, tietoturvallisuuteen, tilaajan aineiston käsittelyyn ja salassapitoon liittyvistä seikoista. Osapuolet tiedostavat, että palveluun sisältyy sellaista tietoa, jonka salassa pysyminen voi olla Tilaajan, Tilaajan kumppanien tai Tilaajan asiakkaiden (potilaiden) turvallisuuden, oikeuksien ja velvollisuuksien kannalta kriittistä. Tällä dokumentilla osapuolet pyrkivät varmistamaan, että salassa pidettävät tiedot pysyvät salassa ja palvelun tuottamisessa noudatetaan tietoturvallisuutta koskevaa lainsäädäntöä. Tässä dokumentissa kuvatuista Palveluntuottajan toimenpiteistä ja velvollisuuksista ei suoriteta erillistä korvausta, ellei toisin ole sovittu sopimuksessa.

1.2. Tätä dokumenttia sovelletaan sopimuksessa mainitun sopimusasiakirjojen soveltamisjärjestyksen mukaisesti, huomioiden kuitenkin mitä jäljempänä mainitaan mahdollisten sopimuksen vastuunrajoitusten soveltamisesta. Tilaajan aineistoa koskevia ehtoja sovelletaan sopimuksen päättymisestä huolimatta niin kauan kuin Palveluntuottajalla on hallussaan tilaajan aineistoa.

2. MÄÄRITELMÄT

Alihankkija tarkoittaa palvelun tuottamiseen osallistuvaa kolmatta osapuolta, jonka toiminnasta Palveluntuottaja vastaa kuin omastaan. Tässä tarkoitetuksi alihankkijaksi katsotaan myös Palveluntuottajan käyttämät ICT-laitteiston huolto- ja korjaustehtäviä suorittavat alihankkijat, ellei toisin sovita.

Asiakastieto tarkoittaa mitä tahansa tietoa, joka: a) viittaa tunnettuun tai tunnistettavaan luonnolliseen tai oikeushenkilöön; b) katsotaan muutoin soveltuvan lain mukaan henkilötiedoksi.

Henkilötieto tarkoittaa kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Määritelty tietosuoja-asetuksen 4 artiklassa.

Käsittely (tietojen käsittely) tarkoittaa tietojen keräämistä, tallettamista, kopiointia, järjestämistä, käyttöä, lukemista, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita tietoihin kohdistuvia toimenpiteitä.

Palvelu tarkoittaa sitä palvelua, josta Tilaaja ja Palveluntuottaja ovat sopineet sopimuksessa.

Poikkeama (tietoturvapoikkeama, tietosuojapoikkeama) tarkoittaa esimerkiksi tahallista tai tahatonta haitallista tapahtumaa tai olotilaa, jonka seurauksena sopimuksen perusteella tuotettavien palvelujen ja Tilaajan vastuulla olevien tietojen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso tai henkilöiden yksityisyyden suoja on tai saattaa olla vaarantunut.

Sopimus tarkoittaa Tilaajan ja Palveluntarjoajan välistä sopimusta sopimusnumero XX/XXXX [Sopimuksen nimi] liitteineen.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Salassa pidettävä tieto tarkoittaa kaikkea sellaista asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä ”julkisuuslaki”) tai muussa lainsäädännössä, ja jonka Tilaaja on tällaiseksi tiedoksi ilmoittanut tai jonka Palveluntuottaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin.

Salassa pidettävää tietoa voivat olla esimerkiksi Tilaajan henkilöstöön, asiakkaisiin, potilaisiin, alihankkijoihin, prosesseihin, palveluihin, tiloihin, tietojärjestelmiin, tietokantoihin, ohjelmistoihin, rekistereihin, turvallisuus- ja varautumisjärjestelyihin sekä liikesalaisuuksiin (ml. tekniset ohjeet) liittyvät tiedot samoin kuin näiden tietojen muotoiluun, rakenteeseen ja metatietoon liittyvät tiedot. Kaikki Tilaajan Palveluntuottajalle luovuttamat henkilötiedot ovat salassa pidettäviä tietoja, ellei Tilaaja toisin kirjallisesti ilmoita.

Salassa pidettävää ei ole tieto, a) joka on yleisesti saatavilla tai julkista tai jonka osapuoli on saanut laillisesti haltuunsa muuten kuin toiselta osapuolelta; b) jonka luovuttamisen ja käyttämisen luovuttaja on nimenomaan hyväksynyt; ja/tai c) joka pakottavan lain, säädöksen tai tuomioistuimen päätöksen tai tuomioistuimen antaman sitovan määräyksen mukaisesti on luovutettavissa olevaa.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Tekninen tukijärjestelmä tarkoittaa pääosin Palveluntuottajan omaan käyttöön tarkoitettua tietojärjestelmää, joka ei sisälly Palvelun toimitukseen, mutta jota Palveluntuottaja käyttää Palvelun tuottamiseen tai jossa käsitellään Tilaajan aineistoa, kuten esimerkiksi sähköposti-, tiketöinti-, työryhmä-, toiminnanohjaus-, konfiguraationhallinta- tai vastaavaa tietojärjestelmää.

Tietojärjestelmä tarkoittaa tiettyä käyttötarkoitusta varten kerätyistä tiedoista muodostettua automaattisen tietojenkäsittelyn avulla yllä pidettyä tiedostoa tai tietovarantoa, jonka avulla käyttäjä voi tuottaa palveluja tai suorittaa muita tehtäviä järjestelmän käyttötarkoituksen ja tietojen käsittelyä koskevien vaatimusten mukaisesti.

Tietotekninen laitetila (IT-laitetila) tarkoittaa erityisesti konesalia, pilvipalvelua, tietoverkon valvomo- ja hallintatilaa tai muuta erillistä teknistä tilaa.

Tilaajan aineisto tarkoittaa sopimuksen ja tämän turvallisuusliitteen mukaisen palvelun yhteydessä käytettävää tai niihin sisältyvää Tilaajan asiakirjaa, kirjallista tietoa, tietokantaa ja ohjelmistoja sekä muuta aineistoa, jonka Tilaaja on luovuttanut Palveluntuottajalle palvelun tuottamista varten sekä lisäksi palvelua käytettäessä syntynyttä Tilaajan tietoaineistoa, tämän muotoilua, rakennetta ja metatietoa.

Tietoaineiston rakenteella ei tarkoiteta tietosisällön tallennusteknistä rakennetta, vaan sen käsitteellistä muotoilua ja jäsennystä Tilaajan tarkoitusta varten. Tietoaineisto voi olla tallennusteknisesti tiedostoissa, tietokannoissa tai muissa tallennusmuodoissa. Tässä määritelmässä tietosisällöllä ja tiedolla tarkoitetaan sekä raakatietoa että jalostettua tietoa.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Toimitila tarkoittaa joko yksittäistä huonetta tai niistä muodostuvaa kokonaisuutta sekä tietoteknisiä laitetiloja, joissa suoritetaan sopimuksessa sovittuja tai siihen liittyviä tehtäviä.

Tietosuoja-asetus: Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

Tietoturvallisuusliite tarkoittaa tätä sopimuksen liitteenä olevaa asiakirjaa.

3. ALIHANKKIJAT

3.1. Mitä tässä tietoturvallisuusliitteessä on määritelty Palveluntuottajasta ja Palveluntuottajan henkilöistä, sovelletaan myös alihankkijaan ja alihankkijan henkilöihin. Mitä tässä tietoturvallisuusliitteessä määritetään alihankkijasta, koskee myös sellaisia Palveluntuottajan alihankintaketjuja ja konserniyhtiöitä, jotka osallistuvat sovitusti Tilaajalle tuotettaviin Palveluihin.

3.2. Palveluntuottaja voi käyttää sopimuksessa tarkoitetun Palvelun tuottamiseen vain Tilaajan hyväksymiä alihankkijoita. Tilaaja ei voi kieltäytyä antamasta hyväksyntäänsä ilman perusteltua syytä. Palveluntuottajalla ei ole oikeutta vaihtaa sopimuksessa nimettyä alihankkijaa tai olennaisten sopimusvelvoitteiden täyttämiseen osallistuvaa alihankkijaa ilman Tilaajan suostumusta.

3.3. Palveluntuottajan tulee huolehtia siitä, että se pystyy noudattamaan tätä tietoturvallisuusliitettä myös käyttäessään alihankkijoita. Palveluntuottajan on tiedotettava alihankkijalleen, että turvallisuusjärjestelyjen saattamisesta tämän tietoturvallisuusliitteen edellyttämälle tasolle saattaa syntyä kustannuksia. Tilaaja ei vastaa näistä kustannuksista.

3.4. Palveluntuottaja vastaa alihankkijoiden ja alihankintaketjun toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän tietoturvallisuusliitteen ehtojen mukaisesti.

3.5. Tilaajan pyynnöstä Palveluntuottajan tulee tehdä tämän tietoturvallisuusliitteen ehtoja vastaava sopimus käyttämänsä alihankkijan kanssa ja Palveluntuottajan on asetettava alihankkijalleen vastaava velvollisuus tämän käyttämän alihankkijan osalta. Mitä tässä sopimuksessa on sovittu Palveluntuottajasta ja Palveluntuottajan henkilöistä, sovelletaan myös alihankkijaan ja alihankkijan henkilöihin. Mitä tässä sopimuksessa sovitaan alihankkijasta, koskee myös sellaisia Palveluntuottajan konserniyhtiöitä, jotka osallistuvat sovitusti Tilaajalle tuotettaviin Palveluihin.

4. SALASSAPITO JA VAITIOLOVELVOLLISUUS

4.1. Tällä tietoturvallisuusliitteellä ei poiketa lainsäädännön asettamista pakottavista velvoitteista. Palveluntuottaja sitoutuu noudattamaan palvelutuotannossaan Suomen lainsäädäntöä.

4.2. Palveluntuottaja sitoutuu pitämään salassa pidettävän tiedon salassa ja käsittelemään sitä lainsäädännön, sopimuksen ja tämän tietoturvallisuusliitteen sekä Tilaajan antamien ohjeiden mukaisesti.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Palveluntuottaja ei käytä tai hyödynnä Tilaajan aineistoa muuhun kuin sopimuksen mukaisen palvelun tuottamiseen siinä laajuudessa kuin se kulloinkin on tarpeen.

4.3. Palveluntuottaja saa luovuttaa Tilaajan aineistoa vain niille henkilöille, jotka tarvitsevat tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Tilaajan aineistoa ei saa oikeudetta näyttää eikä luovuttaa sivulliselle eikä antaa sitä oikeudetta teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi.

4.4. Palveluntuottaja vastaa siitä, että sen palveluksessa olevat henkilöt ovat tietoisia salassapito- ja vaitiolovelvollisuudesta. He eivät saa käyttää hyväksi tuottaessaan sopimuksen mukaista palvelua saamiaan salassa pidettäviä tietoja eivätkä saa niitä ilmaista sivullisille. Salassapito- ja vaitiolovelvollisuus jatkuvat sopimuksen päättymisen jälkeenkin.

4.5. Ellei toisin sovita, Palveluntuottajan henkilön on täytettävä seuraavat edellytykset saadakseen oikeuden käsitellä Salassa pidettävää:

a) Palveluntuottaja on hyväksyttänyt henkilön Tilaajalla etukäteen;
b) henkilö on tietoinen tämän tietoturvallisuusliitteen mukaisista velvoitteistaan; ja
c) henkilö on Tilaajan pyynnöstä allekirjoittanut vaitiolositoumuksen.

4.6. Palveluntuottajan on Tilaajan pyynnöstä laadittava luettelo sellaisista Palvelun tuottamiseen osallistuvista Palveluntuottajan tai sen alihankkijan henkilöistä, joilla on pääsy Tilaajan Salassa pidettävään tietoon. Palveluntuottajan on muutosten tapahtuessa päivitettävä luettelo ja toimitettava se Tilaajalle. Palveluntuottaja luovuttaa Tilaajalle tiedon siitä, ketkä henkilöt käsittelevät palvelun tai järjestelmän tietoturvallisuuden kannalta tärkeää tietoa ja missä roolissa.

4.7. Palveluntuottaja tiedostaa, että salassa pidettävän tiedon luvaton paljastaminen tai oikeudeton käsittely saattaa olla rikoslain mukaan rangaistava teko. Tilaaja valvoo lainsäädännön sallimin keinoin salassapitovelvoitteiden noudattamista.

4.8. Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto.

4.9. Aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Tietojärjestelmien käytön yhteydessä syntyvät tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti. Salassa pidettävien ja arkaluontoisten tietojen hävittäminen suoritetaan niin, että rekisteröityjen yksityisyyttä, etuja ja oikeuksia ei vaaranneta.

4.10. Palveluntuottajalla on nimetty tietoturvavastaava, joka vastaa tietoturvasta ja tekee yhteistyötä Tilaajan tietoturvavastaavan kanssa.

5. TIETOSUOJA

Yleiset velvollisuudet

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

5.1. Osapuolet sitoutuvat noudattamaan tietosuoja-asetusta ja muuta tietosuojasta annettua lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomaismääräyksiä.

5.2. Osapuolet pyrkivät myötävaikuttamaan sopimuksen kohteen toteuttamisessa tietosuojan toteutumista ja luomaan edellytykset toiselle osapuolelle ylläpitää sitä.

5.3. Osapuolet sitoutuvat noudattamaan erityistä huolellisuutta siten, että henkilötietojen luottamuksellisuus, saatavuus tai eheys eivät vaarannu osapuolen henkilöstön huolimattomuuden, virheellisten toimintatapojen tai muun sopimuksen vastaisen toiminnan takia.

5.4. Osapuolet ilmoittavat toiselle osapuolelle ilman aiheetonta viivästystä kaikista sellaisista sopijaosapuolen tietoon tulleista seikoista, jotka voivat vaikuttaa alkuperäiseen sopimuksen liittyvään tietosuojan toteutumisen sekä niiden aiheuttamista toimenpiteistä ja mahdollisista seurauksista.

5.5. Osapuolilla voi olla erillisiä tietosuojaan liittyviä sisäisiä ohjeita. Osapuolten tulee noudattaa niitä siltä osin kuin ne eivät ole ristiriidassa sopimuksen tai tämän tietoturvaliitteen kanssa. Osapuolet pyrkivät mahdollisuuksien mukaan huomioimaan toistensa tietosuojaan liittyvät sisäiset ohjeet.

Osapuolten roolit henkilötietojen käsittelyssä

5.6. Käsiteltäessä henkilötietoja Tilaaja on rekisterinpitäjä ja Palveluntuottaja ovat henkilötietojen käsittelijöitä (jäljempänä myös ”käsittelijä”), ellei henkilötietojen käsittelyn tarkoituksesta muuta johdu. ”Tilaajan henkilötiedoilla” tarkoitetaan näissä ehdoissa henkilötietoja, joista Tilaaja vastaa rekisterinpitäjänä.

5.7. Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän ja käsittelijän velvollisuudet ja oikeudet kuvataan sopimuksen liitteenä olevassa Käsittelytoimien kuvauksessa tai muussa Tilaajan ohjeistuksessa. Palveluntuottaja sitoutuu noudattamaan sopimuksessa, käsittelytoimien kuvauksessa ja ohjeistuksessa olevia ehtoja ja kuvauksia. Tilaaja vastaa ohjeistuksen ylläpidosta ja saatavuudesta.

5.8. Jos kohdan 5.7 mukaista käsittelytoimien kuvausta ei ole tehty tai se on puutteellinen, Tilaaja laatii tai täydentää käsittelytoimien kuvausta tarvittaessa yhteistyössä Palveluntuottajan kanssa.

Palveluntuottajan yleiset velvollisuudet

5.9. Palveluntuottaja noudattaa voimassa olevaa tietosuojalainsäädännön edellyttämiä menettelytapoja ja henkilötietojen käsittelyä ja suojaamista koskevia säännöksiä. Palveluntuottaja vastaa siitä, että palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön ja sopimuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta on säädetty.

5.10. Mikäli Palveluun tai muuhun osapuolen väliseen yhteistyöhön sisältyy henkilötietojen käsittelyä, vastaavat osapuolet omista lakiin perustuvista velvoitteistaan joko rekisterinpitäjänä tai henkilötietojen käsittelijänä.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

5.11. Palveluntuottaja käsittelee henkilötietoja Sopimuksen ja Tilaajan antamien ohjeiden mukaisesti. Ryhmittymän ollessa Käsittelijänä tämän sopimusliitteen velvoitteet koskevat kaikkia ryhmittymän jäseniä, ja ryhmittymän käyttämiä alihankkijoita, jotka osallistuvat henkilötietojen käsittelyyn.

5.12. Palveluntuottaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla se varmistaa, että Tilaajan henkilötietojen käsittely tapahtuu sopimuksen vaatimusten ja sovittujen käytäntöjen mukaisesti. Toimenpiteiden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä käsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus.

5.13. Palveluntuottaja ei käsittele eikä muulla tavoin hyödynnä sopimuksen perusteella käsittelemiään henkilötietoja muutoin kuin sopimuksen täyttämisen mukaisessa tarkoituksessa ja laajuudessa.

5.14. Palveluntuottaja nimeää tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön Tilaajan henkilötietoihin liittyviä yhteydenottoja varten. Palveluntuottaja ilmoittaa kirjallisesti tietosuojavastaavan tai yhteyshenkilön yhteystiedot Tilaajalle.

5.15. Palveluntuottaja saattaa Tilaajan saataville tämän pyynnöstä kaikki tiedot, jotka Tilaaja tarvitsee rekisterinpitäjälle ja Palveluntuottajalle säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja osallistuu pyydettäessä sovitulla tavalla Tilaajan vastuulla olevien kuvausten ja muiden dokumenttien, kuten vaikutustenarvioinnin, laatimiseen ja ylläpitämiseen sekä tietosuoja-asetuksen mukaisen ennakkokuulemisen suorittamiseen. Palveluntuottaja tekee nämä tehtävät sopimuksen mukaisilla hinnoilla, ellei toisin sovita.

5.16. Palveluntuottaja ilmoittaa Tilaajalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Palveluntuottaja ei itse vastaa näihin pyyntöihin. Palveluntuottaja avustaa Tilaajaa, jotta Tilaaja pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyynnöt voivat edellyttää Palveluntuottajalta esimerkiksi avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen. Ellei toisin ole sovittu, Palveluntuottajalla on oikeus laskuttaa Tilaajaa sopimuksessa sovituilla hinnoilla, jos avustaminen aiheuttaa lisäkuluja Palveluntuottajalle. Palveluntuottaja on velvollinen ennakolta ilmoittamaan Tilaajalle mahdollisesti aiheutuvista lisäkuluista.

Henkilötietojen käsittely

5.17. Tilaaja on tietosuojalainsäädännön mukainen rekisterinpitäjä ja Palveluntuottaja henkilötietojen käsittelijä.

Palveluntuottajalla on oikeus käsitellä henkilötietoja

- vain alkuperäisessä sopimuksessa mainitulla perusteella tai tilaajan kirjallisesti etukäteen antamalla luvalla

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

- vain siinä määrin ja niin kauan, kuin se on alkuperäisen sopimuksen kohteen toteuttamiseksi välttämätöntä
- vain tämän ja alkuperäisen sopimuksen sekä tilaajan erikseen antamien dokumentoitujen ohjeiden mukaisesti

Henkilötietojen käsittelyn päättyminen

- Sopimuksen voimassaoloaikana Palveluntuottaja ei saa poistaa Tilaajan lukuun käsittelemiään henkilötietoja ilman Tilaajan nimenomaista pyyntöä.

5.18. Sopimuksen päättyessä tai purkautuessa Palveluntuottaja palauttaa Tilaajalle kaikki Tilaajan puolesta käsitellyt henkilötiedot sekä hävittää omilta taltioiltaan mahdolliset kopiot henkilötiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

6. HALLINNOLLINEN JA FYYSINEN TIETOTURVALLISUUS

Yleiset vaatimukset

6.1. Osapuolet informoivat toista Osapuolta Palvelun tietoturvallisuudesta ja muista vaatimustenmukaisuuteen liittyvistä seikoista pitämällä toisiinsa yhteyttä ja siten, että Osapuolet ovat niistä tarvittavalla tasolla tietoisia tarkemmin myöhemmin kuvattavalla tavalla.

6.2. Palveluntuottaja sitoutuu noudattamaan Tilaajan tietoturvaliitteen vaatimuksia ja tätä täydentäviä erillisiä ohjeistuksia, jotka luovutetaan valitulle Palveluntuottajalle mm. henkilökohtainen käyttäjätunnus, etähallintayhteyskäytäntö ja etähallintayhteyspisteen tekniset vaatimukset. Tilaajalla on oikeus muuttaa, täydentää ja päivittää Palveluntuottajalle antamiaan ohjeita. Jos ohjeiden muutoksista aiheutuu sopimuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovitaan sopimuksen mukaisessa muutoshallintamenettelyssä.

6.3. Palveluntuottaja sitoutuu toteuttamaan riittävät tekniset ja organisatoriset toimenpiteet, joita tarvitaan Tilaajan aineiston suojaamiseksi luvattomalta tietoihin pääsyltä tai tietojen tuhoutumiselta tai muuttumiselta.

6.4. Palveluntuottaja vastaa omalla kustannuksellaan oman henkilökuntansa ja käyttämiensä alihankkijoiden riittävästä kouluttamisesta tietosuojaan ja tietoturvaan liittyvissä asioissa.

6.5. Tilaaja on määrittänyt Palveluun ja Palveluntuottajan toimintaan liittyvät tietoturvavaatimukset, jotka Palveluntuottajan tulee täyttää. Vaatimukset on esitetty Tilaajan hankintakohtaisessa Tietoturva- ja tietosuojavaatimukset -vaatimustaulukossa. Vaatimukset täydentävät tämän tietoturvallisuusliitteen mukaisia vaatimuksia, jotka asettavat vähimmäistason Palvelun tietoturvallisuudelle.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

6.6. Palveluntuottaja on velvollinen ilmoittamaan Tilaajalle, jos Palveluntuottajan on noudatettava Sopimuksen mukaisessa toiminnassaan muuta kuin Suomen tai Euroopan unionin lainsäädäntöä, joka voi muodostaa ristiriidan tämän tietoturvaliitteen tai sopimuksen ehtojen kanssa.

Tilaajan aineiston sijainti

6.7. Tilaajan aineistoa tulee käsitellä EU-lainsäädännön mukaisesti. Ellei palvelun tuottamispaikasta tai Tilaajan aineiston käsittelystä ole toisin sovittu, Palveluntuottajalla on oikeus käsitellä Tilaajan aineistoa ainoastaan Euroopan talousalueella. Palveluntuottaja tiedostaa, että aineiston sijaintia koskevat vaatimukset koskevat myös erilaisia teknisiä tukijärjestelmiä, joita Palveluntuottaja saattaa hyödyntää palvelun tuotannossa.

6.8. Tilaajalla on oikeus rajoittaa Tilaajan aineiston ja sen käsittelyn maantieteellistä sijaintipaikkaa tai tuotantoaluetta. Palveluntuottajalla on velvollisuus ilmoittaa Tilaajalle kaikki ne toimipisteet ja valtiot, joissa se tuottaa palvelua tai käsittelee Tilaajan aineistoa, jos Tilaajaa pyytää tätä tietoa.

6.9. Palveluntuottaja voi siirtää Tilaajan aineistoa sovitusta palvelun tuottamispaikasta ainoastaan Tilaajan etukäteen antaman kirjallisen luvan perusteella. Henkilötietojen siirrossa Sopijapuolet huolehtivat siitä, että siirto toteutetaan tietosuojalainsäädännön mukaisesti. Jos tietosuojalainsäädäntö edellyttää erillistä sopimista, Palveluntuottaja valmistelee kustannuksellaan riittävät tiedonsiirtosopimukset tiedon siirtämiseksi Euroopan talousalueelta kolmansiin maihin tai pääsyn mahdollistamiseksi Euroopan talousalueella olevaan Tilaajan aineistoon Euroopan talousalueen ulkopuolelta. Henkilötietojen siirron osalta hyödynnetään EU:n komission mallisopimuslausekkeita, elleivät sopijapuolet sovi vaihtoehtoisista malleista henkilötietojen lain mukaiseksi siirtämiseksi.

Tilaajan toimitilojen turvallisuus

6.10. Palveluntuottaja vastaa siitä, ettei Tilaajan toimitilojen tai toiminnan turvallisuus vaarannu Palveluntuottajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tietoturvallisuusliitteen vastaisen toiminnan johdosta.

6.11. Ellei toisin sovita, pääsyoikeus muihin kuin Tilaajan julkisiin tiloihin annetaan vain niille Palveluntuottajan henkilöille, jotka

a) Palveluntuottaja on hyväksyttänyt etukäteen,
b) joista on tarvittaessa tehty henkilöturvaselvitys ja tulos on hyväksyttävissä oleva,
c) jotka ovat tietoisia sopimuksen ja tämän tietoturvallisuusliitteen velvoitteista ja tiloissa liikkumisesta annetuista ohjeista.

6.12. Ellei toisin sovita, Palveluntuottajan henkilöstöllä on oltava näkyvillä tunniste, kuten Palveluntuottajan tai Tilaajan myöntämä henkilö- tai vierailijakortti, kun he tuottavat palvelua ja työskentelevät Tilaajan tiloissa.

Palveluntuottajan toimitilojen turvallisuus

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

6.13. Ellei toisin sovita, Palveluntuottajan toimitilat ovat asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi toimitiloihin ja siellä olevaan salassa pidettävään tietoon tietosuojaluokituksen vaatimalla tasolla.

6.14. Ellei toisin sovita, kulunvalvonta Palveluntuottajan IT-laitetiloihin, joissa käsitellään salassa pidettävää tietoa, on järjestettävä siten, ettei kukaan pääse saapumaan tai poistumaan tulematta rekisteröidyksi (sähköinen, kirjallinen loki tai vastaava).

6.15. Palveluntuottajan tulee Tilaajan pyynnöstä hyväksyttää Tilaajalla kaikki henkilöt, joille on tarpeen myöntää pääsyoikeus yksinomaan Tilaajan palvelujen tuottamiseen varattuun Palveluntuottajan tilaan, jossa käsitellään salassa pidettävää tietoa ja joka on sovitulla tavalla eriytetty Palveluntuottajan muusta toiminnasta. Tässä kohdassa tarkoitetuista henkilöistä on Tilaajan niin vaatiessa ja lainsäädännön edellytysten täyttyessä teetettävä henkilöturvallisuusselvitys.

Tietojärjestelmien hallinnan vaatimukset

6.16. Palveluntuottaja on Tilaajan pyynnöstä velvollinen hyväksyttämään Tilaajalla sellaiset Palveluntuottajan henkilöt, jotka voivat pääsyoikeuksiensa perusteella keskeyttää tai vaarantaa Tilaajan tietojärjestelmien toiminnan taikka vaarantaa tietojärjestelmän tietoturvallisuuden. Tilaaja voi hakea tällaisista henkilöistä tarvittaessa henkilöturvallisuusselvityksen.

6.17. Ellei toisin sovita, Palveluntuottajan tulee huolehtia sen vastuulla olevien palveluympäristöjen osalta siitä, että

a) sen henkilöstön oikeudet ja valtuudet palvelun tuottamisessa käytettävissä tietojärjestelmissä rajataan vain työtehtävien edellyttämään laajuuteen,
b) pääsyoikeuksien myöntämisen, muuttamisen ja poistamisen osalta noudatetaan prosessia, joka kattaa toimitilat, tietojärjestelmät ja palvelut,
c) pääsyoikeudet tietojärjestelmiin, joissa käsitellään Tilaajan aineistoa, ovat henkilökohtaisia,
d) mikäli Palveluntuottajan henkilöille myönnetään Tilaajan avaimet, henkilökortit ja kulkuluvat palautetaan ne Tilaajalle sekä käyttäjätunnukset ja pääsyoikeudet poistetaan viivytyksettä, kun henkilö ei enää osallistu palvelun tuottamiseen,

6.18. Sopimuksen päätyttyä Palveluntuottaja palauttaa viivytyksettä Tilaajalle avaimet, henkilökortit, kulkuluvat ja -koodit, salausavaimet, salasanat ja muut tunnistautumisvälineet, mikäli Tilaaja on luovuttanut edellä mainittuja asioita Palveluntuottajalle, ja Tilaajan luovuttaman omaisuuden sekä sulkee tämän sopimuksen nojalla avatut tietoliikenne-, tietojärjestelmä-, tiedonsiirto- ja etäkäyttöyhteydet.

Ohjelmistoturvallisuus

6.19. Palveluntuottaja vastaa Palvelun osalta siitä, että

a) sen toimittamiin tietojärjestelmäpalveluihin, ohjelmistokomponentteihin tai medioihin ei sisälly haittaohjelmia tai muuta tahallista haitallista toiminnallisuutta,

b) se seuraa Palvelun tuottamiseen liittyviin ohjelmistoihin, kolmannen osapuolen komponentteihin ja sen osana oleviin valmisohjelmistoihin liittyviä tietoturvallisuustiedotteita, julkaistuja tietoturvapäivityksiä ja haavoittuvuuksia,
c) se tiedottaa Tilaajaa viivytyksettä Palvelun tuottamiseen liittyvien ohjelmistojen tietoturvahaavoittuvuuksista sekä tietoturvapäivityksistä.

Näillä toimilla varmistetaan Tilaajan aineiston luottamuksellisuus, eheys ja saatavuus sekä palvelun jatkuvuus.

Jatkuvuuden varmistaminen

6.20. Palveluntuottaja vastaa siitä, että sillä on asianmukaiset voimassa olevat suunnitelmat, järjestelyt ja vakuutukset toiminnan jatkuvuuden varmistamiseksi ja suojautumiseen keskeytyksiltä ja jotka on otettu käyttöön. Henkilöstö on harjoitettu ja koulutettu jatkuvuuden varmistamiseen. Palvelun saatavuus, häiriöistä ja vikatilanteista toipumisen prosessit ja niiden tekniset toteutukset on suunniteltu siten, että toiminta pystytään palauttamaan sopimuksen mukaiseksi.

Muutoshallinta ja riskienhallinta

6.21. Palveluihin kohdistuvissa muutoksissa toimitaan sopimuksessa määritellyn muutoshallintamenettelyn mukaisesti.

6.22. Palveluntuottajan on tehtävä tietoturvallisuuteen liittyvien riskien arviointia säännöllisesti ja aina muutostilanteessa.

6.23. Muutosten suunnittelussa huomioidaan aina tietoturvallisuuden vaatimukset. Tilaaja määrittelee tietoturvan vähimmäistason. Palveluntuottaja vastaa Tilaajan määrittelemien vaatimusten toteutuskelpoisen ratkaisun kuvaamisesta ja toteuttamisesta.

7. TURVALLISUUSSELVITYKSET

Tämän tietoturvallisuusliitteen tarkoittamalla turvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain (726/2014) mukaista yritysturvallisuusselvitystä ja henkilöturvallisuusselvitystä taikka niitä vastaavia, Suomen kansallisen turvallisuusviranomaisen (National Security Authority, NSA) kautta hankittua ja ulkomaan turvallisuusviranomaisen myöntämää yritysturvallisuustodistusta ja henkilöturvallisuustodistusta.

Tilaaja määrittää tarjouspyynnössä, tehdäänkö Palveluntuottajasta henkilö- ja yritysturvallisuusselvitykset.

Yritysturvallisuusselvitykset

7.1. Tilaajalla on oikeus hakea Palveluntuottajasta turvallisuusselvityslain mukaisen yritys-turvallisuusselvityksen tai kansainvälisten tietoturvallisuusvelvoitteiden edellyttämän yritysturvallisuusselvityksen (Facility Security Clearance, FSC). Mikäli Palveluntuottajalla on voimassa oleva turvallisuusselvitys, uutta yritysturvallisuusselvitystä ei vaadita uudelleen.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

7.2. Yritysturvallisuusselvityksen hakemisen edellytyksistä on säädetty turvallisuusselvityslain 33 §:ssä. FSC:n hakemisen edellytyksistä on säädetty laissa kansainvälisistä tietoturvavelvoitteista sekä sovittu Suomea sitovissa kansainvälisissä sopimuksissa.

7.3. Yritysturvallisuusselvityksen ja FSC:n edellytyksenä on, että Palveluntuottaja on antanut siihen etukäteisen suostumuksen. Jos Palveluntuottaja kieltäytyy antamasta suostumusta yritysselvityksen hakemiselle, Tilaajalla on sopimuksen mukainen irtisanomisoikeus.

7.4. Turvallisuusselvityslain perusteella tehtävien yritysturvallisuusselvitysten hakemisesta vastaa Tilaaja. Sopijapuolet sopivat erikseen menettelystä FSC:n hankkimiseksi.

7.5. Ellei Sopimuksessa toisin sovita, Palveluntuottaja vastaa kaikista yritysturvallisuusselvitysmenettelyyn (ml. FSC-menettely) liittyvistä kustannuksista. Palveluntuottaja vastaa myös alihankkijansa yritysturvallisuusselvitykseen liittyvistä kustannuksista.

7.6. Jos lainsäädännön tai Suomea velvoittavien sopimusten edellytykset FSC:n hakemiselle eivät täyty sen vuoksi, että Palvelussa ei käsitellä turvallisuusluokiteltua tietoa, mutta Palvelun yhteydessä Palveluntuottaja käsittelee kuitenkin salassa pidettäviä asiakirjoja, Tilaajalla on oikeus pyytää Palveluntuottajaa toimittamaan turvallisuusselvityslain 37 §:ssä säädetyt tiedot Tilaajalle. Tiedot on toimitettava siinä laajuudessa kuin Palveluntuottaja on voimassa olevan lainsäädännön mukaan oikeutettu niitä käsittelemään. Jos Palveluntuottaja kieltäytyy toimittamasta vaadittuja tietoja tämän tietoturvallisuusliitteen mukaisessa laajuudessa, Tilaajalla on sopimuksen mukainen irtisanomisoikeus. Tilaaja on oikeutettu käyttämään toimitettuja tietoja tehdäkseen itse tai toimivaltaisen viranomaisen avustuksella kohdan 7.8 mukaisen arvioinnin. Tilaajan tämän kohdan mukaiseen vaitiolovelvollisuuteen ja hyväksikäyttökieltoon sovelletaan viranomaisten toiminnan julkisuudesta annetun lain 22—24 §:ää.

7.7. Tilaajalla on oikeus arvioida yritysturvallisuusselvityksen sisältö ja yrityksen tai sen vastuuhenkilöiden luotettavuus, yrityksen tietoturvallisuuden taso sekä kyky hoitaa Sopimuksen ja tämän tietoturvallisuusliitteen mukaiset sitoumukset.

Henkilöturvallisuusselvitykset

7.8. Tilaajalla on oikeus hakea turvallisuusselvityslaissa tarkoitettu henkilöturvallisuusselvitys Palveluntuottajan henkilöistä turvallisuuslain mukaisessa laajuudessa. Palveluntuottaja vastaa turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta ja toimittaa henkilön täyttämän ja allekirjoittaman lomakkeen Tilaajalle henkilöturvallisuusselvityksen hakemista varten. Henkilöturvallisuusselvitysten hakemisessa voidaan käyttää mahdollisuuksien mukaan myös sähköistä järjestelmää.

7.9. Ellei toisin sovita, turvallisuusselvityslain mukaista henkilöturvallisuusselvitystä vastaavaksi selvitykseksi hyväksytään toisen valtion antama henkilöturvallisuustodistus (Personal Security Clearance, PSC). Tilaaja voi myös hyväksyä vastaavan toisen valtion viranomaisen tekemän henkilö-turvallisuusselvityksen.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

7.10. Jos henkilöturvallisuusselvitystä tai -todistusta tai PSC-todistusta ei ole saatavissa selvityksen kohteena olevasta henkilöstä, mutta turvallisuusselvityslain mukaiset edellytykset henkilön luotettavuuden ja nuhteettomuuden arvioimiseksi ovat olemassa, Palveluntuottaja toimittaa pyynnöstä kyseisen henkilön rikosrekisteriotteen, liiketoimintakieltorekisteriotteen sekä sakkorekisteriotteen tai vastaavat toisen valtion viranomaisen pitämiin rekistereihin perustuvat otteet Tilaajalle. Tiedot on toimitettava siinä laajuudessa kuin Palveluntuottaja on voimassa lainsäädännön mukaan oikeutettu niitä käsittelemään. Palveluntuottaja on velvollinen hankkimaan selvityksen kohteena olevan henkilön suostumus.

7.11. Tilaaja vastaa henkilöturvallisuusselvityksen kustannuksista. Mikäli ko. selvitys tulee uudelleen tehtäväksi sen vuoksi, että Palveluntuottajan henkilöstössä tapahtuu vaihdos tai Tilaajasta riippumaton lisäys, Palveluntuottaja vastaa kustannuksista.

7.11. Tilaajalla on henkilöturvallisuusselvityksestä tai vastaavasta selvityksestä tai todistuksesta ilmenneestä syystä oikeus olla hyväksymättä Palveluntuottajan ehdottamaa henkilöä sopimuksen mukaisen palvelun tuottamiseen. Tällöin Palveluntuottajan on viivytyksettä ja veloituksetta vaihdettava henkilö. Korvaavalla henkilöllä on oltava vastaava pätevyys ja ammattitaito sekä Tilaajan hyväksyntä. Tilaaja ei saa evätä hyväksyntää ilman pätevää syytä. Palveluntuottajalla ei ole oikeutta laskuttaa kustannuksia, jotka johtuvat uuden henkilön perehdytyksestä palvelun tuottamiseen. Tilaajaan sovelletaan vaitiolovelvollisuutta ja hyväksikäyttökieltoa viranomaisten toiminnan julkisuudesta annetun lain 22 - 24 §:iä.

8. TARKASTAMINEN

8.1. Tilaajalla tai Tilaajalta toimeksi saaneella riippumattomalla kolmannella taholla on oikeus tarkastaa etukäteen ilmoitettuna ajankohtana Palveluntuottajan turvallisuusjärjestelyt sopimuksen mukaisen palvelun tuottamisen osalta.

8.2. Sopijapuolet pyrkivät myötävaikuttamaan tarkastuksen toteuttamista siten, ettei siitä aiheudu kohtuutonta haittaa Palveluntuottajan toiminnalle ja sopimuksen mukaisen palvelun palvelutasolle. Tarkastukset eivät saa vaarantaa Palveluntuottajan tietoturvallisuutta ja Palveluntuottajan salassapitovelvollisuuksia muita asiakkaita kohtaan kuin mikä on välttämätöntä tarkastuksen toteuttamiseksi tietoturvallisuusliitteen vaatimustenmukaisuuden selvittämiseksi.

8.3. Ellei turvallisuusselvityslaista tai auditointilaista muuta johdu tai elleivät sopijapuolet ole toisin sopineet, Tilaaja vastaa tarkastusten ja arviointien ja todistuksen antamisesta aiheutuvista maksuista, kuten tarkastajan työkustannuksesta. Selvyyden vuoksi todetaan, että Palveluntuottaja vastaa kaikista niistä kuluista ja kustannuksista, joita sille tai sen alihankkijalle aiheutuu tarkastuksiin käytetystä työajasta, havaittujen puutteiden korjaamisesta ja kuluista, jotka aiheutuvat Palvelun saattamiseksi sovittujen vaatimusten mukaisiksi.

8.4. Ellei toisin ole sovittu, Tilaajan on ilmoitettava tahdostaan suorittaa tarkastus viimeistään neljätoista (14) päivää ennen ehdotettua tarkastuspäivää. Palveluntuottaja voi ehdottaa uutta päivää tarkastukselle.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Uusi päivä ei kuitenkaan saa olla myöhemmin kuin 10 (päivää) Tilaajan ilmoittaman päivän jälkeen. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainitusta määräajasta riippumatta erikseen sovittavina ajankohtina.

8.5. Palveluntuottajan tulee huolehtia sopimusjärjestelyin siitä, että Tilaajalla on mahdollisuus tarkastaa Palveluntuottajan alihankkijan tai alihankintaketjun turvallisuusjärjestelyt.

8.6. Jos tarkastuksessa havaitaan, ettei Palveluntuottajan toiminta täytä sovittuja vaatimuksia, Palveluntuottaja laatii viipymättä aikataulutetun suunnitelman tilanteen korjaamiseksi ilman eri veloitusta. Ellei sopijapuolten hyväksymästä suunnitelmasta muuta johdu, Palveluntuottajan tulee korjata tarkastuksessa havaitut puutteet viivytyksettä Tilaajan kirjallisesta ilmoituksesta. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvallisuudelle, on korjattava heti tai Tilaajan asettamassa aikataulussa. Tilaaja ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.

8.7. Mikäli tarkastuksessa havaitaan, ettei Palveluntuottajan toiminta täytä sovittuja vaatimuksia ja Tilaaja edellyttää virheen korjaamisen todentamiseksi uusintatarkastusta, Palveluntuottaja korvaa Tilaajalle uusintatarkastuksesta aiheutuneet kustannukset.

8.8. Tilaajalla on oikeus tehdä tässä kohdassa tarkoitettu tarkastus myös sopimuksen päättymisen jälkeen. Tilaaja voi tarkastaa erityisesti sen, että Palveluntuottaja on tuhonnut tietoturvallisesti kaiken Sopimuksen perusteella käsittelemänsä Tilaajan aineiston.

8.9. Tilaajalla on oikeus luovuttaa muille viranomaisille tieto siitä, että tämän luvun mukainen tarkastus on suoritettu ja siitä, ovatko Palveluntuottajan turvallisuusjärjestelyt todettu vaatimusten mukaisiksi. Tilaajalla ei kuitenkaan ole ilman Palveluntuottajan lupaa oikeutta luovuttaa tietoa tarkastuksen yksityiskohtaisista havainnoista, ellei pakottavasta lainsäädännöstä muuta johdu.

9. RAPORTOINTI JA VIESTINTÄ

9.1. Palveluntuottaja on velvollinen kirjallisesti ilmoittamaan Tilaajalle, jos Palveluntuottajan tai sen alihankkijan tämän turvallisuusliitteen kannalta keskeisissä toiminnoissa tapahtuu olennaisia muutoksia tai jos Palveluntuottajan tai sen alihankkijan määräämisvallassa taikka yhtiörakenteessa tapahtuu muutoksia. Määräysvallan muutosta arvioidaan kirjanpitolain (1336/1997) 1 luvun 5 §:n perusteella.

9.2. Palveluntuottaja on tietoinen ulkomaalaisten yritysostojen seurannasta annetun lain (172/2012) mukaisista velvoitteista. Sen lisäksi mitä sanotussa laissa säädetään yritysoston ilmoittamisesta toimivaltaiselle viranomaiselle, Palveluntuottaja ilmoittaa Tilaajalle lain 2 §:n 1 momentin 5 kohdassa tarkoitetusta yritysostosta viipymättä yritysoston toteutumisen jälkeen ja antaa Tilaajalle tarvittavat tiedot ulkomaisesta omistajasta sekä yritysoston keskeisestä sisällöstä.

9.3. Palveluntuottaja valvoo tämän tietoturvallisuusliitteen edellyttämän turvallisuustason toteutumista ja vaatimuksen mukaisuutta toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

ja raportoi ne Tilaajalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Palveluntuottaja ei veloita tämän kohdan mukaisista toimenpiteistä, ellei toisin ole sovittu.

9.4. Palveluntuottaja on viipymättä velvollinen ilmoittamaan Tilaajalle, mikäli Palveluntuottajaan kohdistuu Tilaajaa mahdollisesti uhkaavia yhteydenottoja tai uhkatilanteita.

9.5. Osapuolet seuraavat tietoturvallisuuteen ja ICT-varautumiseen liittyviä muutoksia ja ilmoittavat toiselle osapuolelle muutostarpeista. Muutosten toteuttamisesta ja kustannuksista sovitaan erikseen.

9.6. Tilaaja vastaa omaan toimintaansa liittyvästä viestinnästä. Osapuolet voivat tehdä Palvelun osalta viestintäsuunnitelman.

9.7. Ellei toisin sovita, Palveluntuottajan on toimitettava Tilaajan hyväksyttäväksi Palveluntuottajan sisäisille tai ulkoisille sidosryhmille osoitettavat julkaisut tai markkinointimateriaali, jotka liittyvät Sopimuksen mukaiseen yhteistyöhön. Edellä sovittua ei kuitenkaan sovelleta pörssitiedotteisiin tai muihin vastaaviin lainsäädäntöön perustuviin tiedottamisvelvoitteisiin.

9.8. Palveluntuottajalla on velvollisuus huolehtia käyttölokituksesta ja raportoida Tilaajalle yhdessä sovitun käytännön mukaisesti säännöllisesti ja/tai pyydettäessä.

9.9. Kaikki tiedot, raportit ja selosteet ja muut sopimuksen mukaiset palvelut tulee toimittaa Tilaajalle tietoturvallisesti esimerkiksi käyttämällä suojattua sähköpostia tai muuta yhteisesti sovittua kanavaa, joka täyttää vaatimukset tietoturvallisesta tietojen toimittamisesta. Toimittamistapa sovitaan erikseen, kun palvelun tuottaminen on aloitettu.

10. TIETOTURVALOUKKAUSTEN KÄSITTELY

10.1. Palveluntuottajalla tulee olla kirjallinen ohjeistus tietosuojaloukkaustilanteissa toimimiseen.

10.2. Palveluntuottaja ilmoittaa Tilaajalle välittömästi ja viimeistään 24 tunnin kuluessa sen tietoon tulleesta Tietoturvaloukkauksesta. Ilmoitus tulee tehdä kirjallisesti. 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.

10.3. Lisäksi Palveluntuottaja sitoutuu ilmoittamaan Tilaajalle muista Palveluntuottajan tuottaman palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia Tilaajan Salassa pidettävien tietojen luottamukselliselle käsittelylle tai sellaisten henkilöiden asemaan ja oikeuksiin, joiden henkilötietoja Palveluntuottaja käsittelee. Ilmoitus on tehtävä ilman aiheetonta viivytystä.

10.4. Palveluntuottajan on annettava Tilaajalle vähintään seuraavat tiedot tietoturvaloukkauksesta:

a) kuvattava tietoturvaloukkaus; mikäli kyseessä on henkilötietoihin kohdistunut tietoturvaloukkaus, kuvattava mahdollisuuksien mukaan myös asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

b) ilmoitettava tietosuojavastaava tai muu vastuuhenkilö, jolta voi saada asiassa lisätietoja;
c) kuvattava tietoturvaloukkauksen todennäköiset seuraukset; sekä
d) kuvattava toimenpiteet, joita Palveluntuottaja ehdottaisi tai joita se on toteuttanut tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

10.5. Tietoturvaloukkauksen havaittuaan Palveluntuottaja ryhtyy viipymättä sopimuksessa sovittuihin toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.

10.6. Rikos- ja väärinkäyttötapauksissa tai sellaisia epäiltäessä Osapuolet pyrkivät olosuhteet ja lainsäädännön vaatimukset huomioon ottaen neuvottelemaan jatkotoimenpiteistä. Osapuolilla on velvollisuus avustaa toisiaan asian selvittämisessä viranomaistahojen kanssa.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi