Etelä-Pohjanmaan hyvinvointialue Tietoturvallisuusliite

4.11.2022

Etelä-Pohjanmaan hyvinvointialue ja

[Palveluntuottaja]

ISBN 952-452-059-1
ISSN 1796-

Etelä-Pohjanmaan hyvinvointialue

Sisällys

1. Johdanto

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 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.

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. Alihankkijat

Mitä tässä tietoturvallisuusliitteessä on määritelty Palveluntuottajasta ja Palveluntuottajan henkilöistä, sovelletaan myös alihankkijaan ja alihankkijan henkilöihin.

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.

Palveluntuottajan tulee huolehtia siitä, että se pystyy noudattamaan tätä tietoturvallisuusliitettä myös käyttäessään alihankkijoita. Palveluntuottaja vastaa alihankkijoiden ja alihankintaketjun toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän tietoturvallisuusliitteen ehtojen mukaisesti.

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 alihank**kijaan ja alihankkijan henkilöihin.**

3. Salassapito ja vaitiolovelvollisuus

Tällä tietoturvallisuusliitteellä ei poiketa lainsäädännön asettamista pakottavista velvoitteista.

Palveluntuottaja sitoutuu noudattamaan palvelutuotannossaan Suomen lainsäädäntöä huomioiden erityisesti seuraavat lait ja asetukset: tietosuojalaki (1050/2018), laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), laki potilaan asemasta ja oikeuksista (785/1992), laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000), laki viranomaisten toiminnan julkisuudesta (621/1999), laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009), laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009), arkistolaki (831/1994), tiedonhallintalaki (906/2019) ja laki sosiaalihuollon asiakasasiakirjoista (254/2015) sekä sosiaali- ja terveysministeriön asetus potilasasiakirjoista (asetus potilasasiakirjoista 298/2009), sosiaali- ja terveysministeriön asetus valtakunnallisista tietojärjestelmäpalveluista (1257/2015), EU:n tietosuoja-asetus (EU 2016/679) ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021).

Palveluntuottaja sitoutuu pitämään salassa pidettävän tiedon salassa ja käsittelemään sitä lainsäädännön, sopimuksen ja tämän tietoturvallisuusliitteen sekä Tilaajan antamien ohjeiden mukaisesti eikä käytä tai hyödynnä aineistoa muuhun kuin sopimuksen mukaisen palvelun tuottamiseen.

Palveluntuottaja saa luovuttaa Tilaajan aineistoa vain niille henkilöille, jotka tarvitsevat tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Tilaajan aineistoa ei saa oikeudetta näyttää eikä luovuttaa sivulliselle.

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.

Ellei toisin sovita, Palveluntuottajan henkilön on täytettävä seuraavat edellytykset saadakseen oikeuden käsitellä salassa pidettävät asiakirjat ja on tietoinen tämän tietoturvallisuusliitteen mukaisista velvoitteistaan.

Palveluntuottaja tiedostaa, että salassa pidettävän tiedon luvaton paljastaminen tai oikeudeton käsittely saattaa olla rikoslain mukaan

rangaistava teko. Tilaaja valvoo lainsäädännön sallimin keinoin salassapitovelvoitteiden noudattamista.
Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto.

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.

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

4. Tietosuoja

Yleiset velvollisuudet

Sopijapuolten velvollisuus noudattaa lainsäädäntöä: Osapuolet sitoutuvat noudattamaan tietosuoja-asetusta ja muuta tietosuojasta annettua lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomaismääräyksiä. Osapuolet sitoutuvat noudattamaan myös tietosuojalainsäädäntöä täydentävää tiedonhallintalakia (906/2019) sekä ottamaan erityisellä tavalla huomioon tiedon elinkaaren merkitys.

Myötävaikutusvelvollisuus: Osapuolet pyrkivät kaikin käytettävissään olevin kohtuullisin keinoin myötävaikuttamaan sopimuksen kohteen toteuttamisessa korkeaan tietosuojan tasoon ja toisen osapuolen mahdollisuuteen omalta osaltaan ylläpitää sitä.

Huolellisuusvelvollisuus: Osapuolet vastaavat siitä, että sopimuksen mukaiset tehtävät tehdään huolellisesti ja ettei henkilötietojen luottamuksellisuus, saatavuus tai eheys vaarannu osapuolten henkilöstön huolimattomuuden, virheellisten työtapojen tai muun sopimuksen vastaisen toiminnan johdosta.

Ilmoitusvelvollisuus: Osapuolen on viipymättä ilmoitettava toiselle osapuolelle sellaisista sopijapuolen tietoon tulleista seikoista, jotka voivat vaikuttaa alkuperäiseen sopimukseen liittyvään tietosuojaan, sekä niiden aiheuttamista toimenpiteistä ja mahdollisista seurauksista. Ilmoituksen tulee mahdollisuuksien mukaan sisältää asiaan liittyvien rekisteröityjen ryhmät ja arvioidut lukumäärät.

Sopijapuolten tietosuojaan liittyvät sisäiset ohjeet: 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.

Palveluntuottajan yleiset velvollisuudet

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.

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

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.

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.

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

5. Tarkastaminen

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

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.

Ellei turvallisuusselvityslaista tai auditointilaista muuta johdu tai elleivät sopijapuolet ole toisin sopineet, Tilaaja vastaa tarkastus-

ten 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.

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

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

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.

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

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.

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.

6. Raportointi ja viestintä

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.

Palveluntuottaja valvoo tämän tietoturvallisuusliitteen edellyttämän turvallisuustason toteutumista ja vaatimuksen mukaisuutta toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Tilaajalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Palveluntuottaja ei veloita tämän kohdan mukaisista toimenpiteistä, ellei toisin ole sovittu.

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.

7. Tietoturvaloukkausten käsittely

Palveluntuottajalla tulee olla kirjallinen ohjeistus tietosuojaloukkaustilanteissa toimimiseen.

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.

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.

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;

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 tietoturvaloukkauksenjohdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

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

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