TIETOTURVALLISUUSSITOUMUS

Palvelusetelisääntökirjan yleisen osan liite

Sisällysluettelo

1 MÄÄRITELMÄT

”Alihankkija” tarkoittaa mitä tahansa Palvelun tuottamiseen tai yhteistyöhön muuten osallistuvaa osapuolta, jota Palveluntuottaja käyttää omien velvoitteidensa täyttämiseksi.

”Henkilötietojen tietoturvaloukkaus” (Personal Data Breach) tarkoittaa tietosuoja-asetuksen 14 artiklan 12) kohdan mukaan Tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

”Palvelu” tarkoittaa palvelusetelisääntökirjan mukaista Palvelua, josta asiakas ja Palveluntuottaja ovat sopineet.

”Tietoaineisto” tarkoittaa tähän Palveluun liittyvää Hyvinvointialueen asiakirjoista ja muista tiedoista muodostuvaa tietokokonaisuutta.

”Tietojärjestelmä” tarkoittaa tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä.

”Tietosuojalainsäädäntö” tarkoittaa, rajoituksetta ja soveltuvin osin, kaikkea kulloinkin voimassa olevaa henkilötietojen suojaan liittyvää EU-lainsäädäntöä ja kansallista lainsäädäntöä, kuten EU:n yleistä tietosuoja-asetusta (TSA, 679/2016) sekä kansallista tietosuojalakia (1050/2018).

”Tietoturvatapahtuma” on yksittäinen tapahtuma, joka saattaa vaikuttaa tietoturvaan

”Tietoturvapoikkeama” tai **”Tietoturvahäiriö”** on yksi tai useampi tietoturvatapahtuma, vaarantaen tietoturvan ja vaikuttaen organisaation toimintaan

”Tietoturvaloukkaus” oikeudeton puuttuminen tietoon.

”Hyvinvointialue” (Kanta-Hämeen hyvinvointialue), joka asettaa Palvelun vaatimukset ja hyväksyy niiden täyttymisen.

“Hyvinvointialueen aineisto” tai **Hyvinvointialueen tieto”** tarkoittaa kaikkea Hyvinvointialueen Palveluntuottajalle luovuttamaa tai Palveluntuottajalla olevaa tai Palveluntuottajan laatimaa tietoa, joka liittyy hankinnan kohteena olevan palvelun tuottamiseen.

”Tilat” tarkoittavat sellaisia Palveluntuottajan tai sen Alihankkijan tiloja, joissa säilytetään tai muutoin käsitellään Tietoaineistoja.

”Palveluntuottaja” Hyvinvointialueen hyväksymä palvelusetelituottaja, jonka tuottamien palvelujen maksamiseen asiakas voi käyttää palveluseteliä.

Sitoumukseen sovelletaan lisäksi EU:n yleisen tietosuoja-asetuksen (2016/679, myös TSA) määritelmiä.

2 TAUSTA JA TARKOITUS

Tässä sitoumuksessa sovitaan Palveluntuottajan noudatettavista turvallisuusjärjestelyistä sekä Tietoaineistojen käsittelyä koskevista käytännöistä. Ehtoja sovelletaan Palveluiden tuottamisessa sekä kaikessa Hyvinvointialueen ja Palveluntuottajan välisessä yhteistyössä.

3 TIETOTURVALLISUUDEN HALLINTA

Palveluntuottajalla on tietoturvallisuusperiaatteet, jotka kuvaavat Palveluntuottajan tietoturvallisuustoimenpiteiden kytkeytymisen organisaation toimintaan.

Palveluntuottaja on määritellyt tietoturvallisuuden hoitamiseen liittyvät tehtävät ja vastuut sekä huolehtii henkilöstönsä säännöllisestä tietoturvallisuuskoulutuksesta.

Palveluntuottajalla on tietoturvallisuuteen liittyvien poikkeamatilanteiden käsittelyyn määritellyt prosessit ja toimintaohjeet.

4 TIETOAINEISTOJEN KÄSITTELY

Tässä Tietoturvallisuusliitteessä kuvattuja järjestelyjä noudatetaan aina Palveluntuottajan käsitellessä Asiakkaaseen tai Palvelun tuottamiseen liittyvää tai muuta Hyvinvointialueelta saatua Tietoaineistoa Palveluntuottajan tuottaessa Sopimuksen mukaista Palvelua ja Asiakkaalle. Palveluntuottaja käsittelee Tietoaineistoja vain Palvelun tuottamisen edellyttämässä laajuudessa.

Palveluntuottaja antaa Hyvinvointialueen tietoja vain niille henkilöille, jotka tarvitsevat tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Palveluntuottajan tulee pystyä osoittamaan, että sen Palvelun tuottamiseen osallistuvat henkilöt ovat tietoisia tämän liitteen mukaisista vaatimuksista ja vaitiolovelvollisuudesta. Palveluntuottaja toimittaa Hyvinvointialueen pyynnöstä selvityksen tämän kohdan mukaisen velvollisuuden täyttämisestä.

Palveluntuotannon päätyttyä Palveluntuottaja palauttaa Tietoaineiston yleisesti käytössä olevassa muodossa tai tuhoaa Tietoaineiston siten, ettei tietoja ole enää mahdollista palauttaa luettavaan muotoon. Palveluntuottajalla on oikeus säilyttää tietoaineistoja säädösten ja viranomaismääräysten edellyttämällä tavalla.

5 PÄÄSY TIETOJÄRJESTELMIIN JA TIETOIHIN

Palveluntuottajan ja sen Alihankkijan Tilojen tulee olla asianmukaisesti suojattu siten, etteivät ulkopuoliset pääse käsiksi tietoihin. Palveluntuottaja antaa pääsyn Tietoaineistoihin ja näitä käsitteleviin tietojärjestelmiin vain nimetyille henkilöille.

6 LOKITIEDOT

Lokitiedot ovat Hyvinvointialueen aineistoa siltä osin kuin lokituksen kohteena on Hyvinvointialueen aineiston käsittely tai luovuttaminen. Siltä osin kuin lokitiedot ovat Hyvinvointialueen aineistoa, Palveluntuottajan tulee toimittaa lokitiedot Hyvinvointialueen pyynnöstä ja ilman erillistä korvausta Hyvinvointialueelle. Hyvinvointialue voi myös erikseen edellyttää säännöllistä raportointia lokitiedoista.

Mikäli lokitiedot sisältävät henkilötietoja, lokitietojen käsittelyyn sovelletaan Tietolainsäädäntöä.

Siltä osin kuin lainsäädännössä tai viranomaismääräyksissä on säädetty lokitietojen käsittelystä, sovelletaan ensisijaisesti kyseisiä säädöksiä ja viranomaismääräyksiä.

Lokitiedot ovat viranomaisen toiminnan julkisuudesta annetun lain (621/1999) 24 § 1 mom 7 kohdan 24 §:n mukaisesti salassa pidettäviä.

Järjestelmän tulee kerätä tiedonhallintalain (906/2019) 17 §:ssä tarkoitetut käyttö- ja luovutuslokitiedot silloin, kun jokin seuraavista ehdoista täyttyy:

- käsitellään henkilötietoja, ja
- käsitellään salassa pidettäviä tietoja,

tai

- lokitiedot ovat tarpeen käyttäjien oikeusturvan ja vastuun kannalta tai
- lokitiedot ovat tarpeen teknisten virheiden selvittämiseksi.

7 TIETOSUOJA

Palveluntuottajan tulee kaikessa toiminnassaan noudattaa voimassa olevaa Tietosuojalainsäädäntöä.

Palveluntuottaja vastaa siitä, että Asiakkaille tuotettu Palvelu on kulloinkin voimassa olevan Tietosuojalainsäädännön vaatimusten mukainen, ottaen erityisesti huomioon oletusarvoisen ja

sisäänrakennetun tietosuojan periaatteet. Palveluntuottaja huolehtii käsittelemiensä tietojen asianmukaisesta suojaamisesta varmistaakseen Hyvinvointialueen aineiston luottamuksellisuuden, eheyden ja saatavuuden.

Mikäli Henkilötietojen käsittelijä siirtää henkilötietoja EU:n tai ETA-alueen ulkopuolelle kolmansiin maihin, henkilötietojen siirto tulee tehdä asianmukaisella siirtosopimuksella noudattaen EU-komission kulloinkin voimassa olevia mallilausekkeita ja voimassa olevia henkilötietojen siirtoa koskevia vaatimuksia.

Henkilötietojen käsittelijän tulee avustaa Rekisterinpitäjää varmistamaan, että tietosuoja-asetuksen 3 luvussa sekä 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan. Henkilötietojen käsittelijän tulee esimerkiksi avustaa Rekisterinpitäjää tietosuoja-asetuksen 33 ja 34 artiklan edellyttämien ilmoitusten tekemisessä tietosuoja-asetuksen mukaisessa määräajassa valvontaviranomaiselle ja rekisteröidylle. Henkilötietojen käsittelijän tulee myös pyynnöstä tehdä tietosuoja-asetuksen 31 artiklan mukaista yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

Selvyyden vuoksi todetaan, että tässä Sitoumuksessa mainittu Hyvinvointialue on tämän Sitoumuksen mukaista Palvelua koskevien henkilötietojen osalta tietosuoja-asetuksessa tarkoitettu rekisterinpitäjä ja Palveluntuottaja henkilötietojen käsittelijä.

8 SELOSTE KÄSITTELYTOIMISTA

Henkilötietojen käsittelijä ylläpitää tietosuoja-asetuksen 30 artiklan mukaista sähköistä selostetta Rekisterinpitäjän lukuun suorittamastaan henkilötietojen käsittelystä.

Henkilötietojen käsittelijän selosteen tulee sisältää vähintään seuraavat tiedot:

1. Rekisterinpitäjän ja sen tietosuojavastaavan nimi ja yhteystiedot;
2. Henkilötietojen käsittelijän ja sen tietosuojavastaavan nimi ja yhteystiedot;
3. kuvaus Henkilötietojen käsittelijän Rekisterinpitäjän lukuun käsittelemistä rekisteröityjen ryhmistä ja henkilötietoryhmistä;
4. tiedot mahdollisista henkilötietojen siirroista EU- tai ETA-alueen ulkopuolelle;
5. lista henkilötietojen käsittelyssä käytetyistä alikäsittelijöistä; sekä
6. kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista toimenpiteistä.

Rekisterinpitäjä ja Henkilötietojen käsittelijä käyvät edellä mainittua selostetta yhdessä läpi tarvittaessa.

9 OHJE HENKILÖTIETOJEN TIETOTURVALOUKKAUKSIEN SELVITTÄMISESTÄ

EU:n yleisen tietosuoja-asetuksen mukaan 33 ja 34 artiklojen mukaan Rekisterinpitäjän on ilmoitettava henkilötietoihin kohdistuneesta tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta tietosuojavaltuutetulle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, Rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

Jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Henkilötietojen käsittelijän tulee ilmoittaa kirjallisesti tietoturvaloukkauksesta Rekisterinpitäjälle (Kanta-Hämeen hyvinvointialue) ilman aiheetonta viivytystä saatuaan sen tietoonsa ja 36 h määräajassa, jollei ole erikseen sovittu, että Henkilötietojen käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan valvontaviranomaiselle asetuksen edellyttämällä tavalla. Vastuu ilmoitusvelvollisuuden toteuttamisesta säilyy kuitenkin Rekisterinpitäjällä.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt USB-tikku, varastettu tietokone, hakkerointi, haittaohjelmatartunta, arkaluontoisia henkilötietoja löytyy roskalavalta, kyberhyökkäys, tulipalo datakeskuksessa tai tiliotteen postitus väärälle henkilölle.

10 SALASSAPITO JA HUOMIOON OTETTAVA LAINSÄÄDÄNTÖ

Tietojen käsittelyoikeus koskee vain työtehtävien edellyttämiä tietoja. Henkilötietojen käsittely perustuu aina toimeksiantoon. Henkilötietoja ei saa käsitellä muuhun kuin laissa tai muuten sovitusti määriteltyyn käyttötarkoitukseen.

Palvelusetelituottajuuden aikana tai sen päätyttyä sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja Kanta-Hämeen hyvinvointialuetta tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia lain mukaan salassa pidettäviä tai muuten vaitiolovelvollisuuden piirissä olevia tietoja. Tällaisia tietoja ovat mm. Kanta-Hämeen hyvinvointialueen ja sen sopimustoimittajien liikesalaisuudet, kaikki arkaluonteiset ja erityisiä henkilötietoryhmiä koskevat henkilötiedot sekä mahdollisesti tietoon tulleet käyttäjien sähköpostien sisällöt, lokitiedot tms. Näitä tietoja ei saa väärinkäyttää tai jättää paikkaan, jossa ne ovat sivullisten nähtävillä tai saatavilla.

Hyvinvointialueen ulkopuolinen taho, jolla on Kanta-Hämeen hyvinvointialueen kanssa tehtyyn toimeksiantoon perustuva pääsy hyvinvointialueen tietojärjestelmiin ja/tai salassa pidettävään tietoon, noudattaa tätä liitettä ja laissa säädettyjä kulloinkin voimassa olevia vaitiolovelvollisuus- ja hyväksikäyttökieltosäännöksiä sekä muita salassapitoa, tietosuojaa ja tietoturvaa koskevia säännöksiä. Näitä säännöksiä on erityisesti seuraavissa laeissa ja määräyksissä:

- EU yleinen tietosuoja-asetus (2016/679)

- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Tietosuojalaki (1050/2018)
- Tiedonhallintalaki (906/2019)
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023), lisäksi
  - THL määräys 3/2024
  - THL määräys 4/2021
  - THL määräys 5/2021
- Liikesalaisuuslaki (595/2018)
- Laki sähköisen viestinnän palveluista (917/2014)
- Rikoslaki, 38 luku (39/1889)
- Tekijänoikeuslaki (404/1961)
- Lakiammatillisesta koulutuksesta (2017/517)
- Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
- Laki vesi- ja energiahuollon, liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja käyttöoikeussopimuksista (1398/2016)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018)
- Turvallisuusluokitteluasetus (1011/2019)
- Varhaiskasvatuslaki (540/2018)

Selvyyden vuoksi todetaan, että em. lakien osalta toimitaan vain soveltuvilta osin eli huomioiden yhteistyön luonne.

11 MUUT OIKEUDET JA VELVOLLISUUDET

- Tietojärjestelmää saa käyttää vain henkilökohtaisella käyttäjätunnuksella.
- Tunnistautumisen tulee tapahtua Hyvinvointialueen hyväksymällä vahvalla tunnistautumisella.
- Hyvinvointialueen erillisellä luvalla vahvasta tunnistautumisesta voidaan poiketa.
- Jokainen työntekijä vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja toimenpiteistä.
- Käyttäjätunnusta ja salasanaa ei saa antaa muiden tietoon.
- Käyttöoikeuksiin liittyvissä tehtävissä lokitietoja on käsiteltävä siten, ettei yksityisyyden suoja tai tietosuoja miltään osin vaarannu.
- Tietojärjestelmien käyttöä seurataan ja niiden käytöstä kertyy lokitietoja.
- Ylläpitäjä saattaa ylläpitotehtäviä hoitaessaan saada tietoja viesteistä ja tunnistamistiedoista. Viestin sisältöä tai tietoa viestin olemassaolosta ei saa ilmaista muille tai käyttää hyväksi ilman viestinnän osapuolen suostumusta, ellei laissa toisin säädetä.
- Ylläpitäjällä on oikeus tutustua tai muulla tavoin puuttua käyttäjien verkkoliikenteen sisältöön ja tiedostoihin ilman käyttäjältä saatua lupaa vain palvelun toteuttamiseksi tai

käyttämiseksi ja tietoturvasta huolehtimiseksi, viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi, väärinkäytösten havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi.

- Palvelusetelituottajuuden päättyessä kaikki Kanta-Hämeen hyvinvointialuetta tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevat tiedot tai asiakirjat ja tietovälineet sekä niiden mahdolliset kopiot luovutetaan Kanta-Hämeen hyvinvointialueelle, ellei lainsäädännöstä muuta johdu tai asiasta muuta sovita.
- Kun tiedot tai asiakirjat on Kanta-Hämeen hyvinvointialueelle luovutettu ja Kanta-Hämeen hyvinvointialueen osalta luovutus on hyväksytty, Palveluntuottajan on hävitettävä kaikki omat kappaleensa, ellei lainsäädännöstä muuta johdu, tiedoista ja asiakirjoista tietokannoistaan ja muista tietovälineistä todennetusti siten, että Kanta-Hämeen hyvinvointialue on sen hyväksynyt.

12 SEURAAMUKSET

Sääntöjen ja periaatteiden rikkomisesta tietojärjestelmien käyttöoikeudet voidaan peruuttaa. Rikkomuksista tiedotetaan aina toiselle osapuolelle ja ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli rikkomuksesta aiheutuu välitöntä tai välillistä taloudellista vahinkoa tai henkilötietojen vuotoja, sovelletaan sovellettavan lainsäädännön mukaisia oikeussuojakeinoja. Tietojen väärinkäyttö voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

13 ALIHANKKIJAT

Mitä tässä liitteessä on sovittu Palveluntuottajan henkilöstöstä, sovelletaan myös Alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön. Palveluntuottaja vastaa siitä, että sen Alihankkijat toimivat tämän liitteen vaatimusten mukaisesti ja toimittaa Hyvinvointialueen pyynnöstä selvityksen tämän kohdan mukaisen velvollisuuden täyttämisestä.

14 RAPORTOINTI

Palveluntuottaja on velvollinen ilmoittamaan Hyvinvointialueelle välittömästi, jos Palveluntuottajan tai sen Alihankkijan keskeisissä turvallisuustoiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia. Palveluntuottaja valvoo näiden ehtojen edellyttämien järjestelyjen tason toteutumista toiminnassaan säännöllisesti, kirjaa mahdolliset poikkeamat ja raportoi merkittävistä poikkeamista Hyvinvointialueelle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa.

Palveluntuottaja toimittaa Hyvinvointialueen pyynnöstä selvityksen tämän Tietoturvallisuussitoumuksen mukaisten velvollisuuksien täyttämisestä.

15 VOIMAAN JÄÄVÄT EHDOT

Tämän sitoumuksen ehdot ovat voimassa viisi (5) vuotta palvelusetelituottajuuden päättymisen jälkeen, ellei lainsäädännöstä muuta johdu.

Tämän sitoumuksen salassapitoa koskevat ehdot jatkuvat palvelusetelituottajuuden päättymisen jälkeen pysyvästi.