

Palvelutuotannon tietoturva- ja tietosuojasitoumus

1. Salassapito palvelutuotannossa digitaalisenturvallisuuden varmistamiseksi

Salassapitovelvollisuudesta (asiakirjasalaisuus ja vaihteluvelvollisuus) säädetään yleislaeissa sekä sosiaali- ja terveyshuollon ja pelastustoimen erityislaeissa. Potilas- ja asiakastiedot ovat terveyden- ja sosiaalihuollon erityislainsäädännön mukaisesti salassa pidettäviä. Pelastuslain (379/2011) luvussa 13 pykälissä 86 ja 107 määrätään vaihteluvelvollisuudesta sekä salassapidosta pelastustoimissa

Tässä sitoumuksessa ei ole erikseen lueteltu kaikkia yleislakeja eikä pelastustoimen tai sosiaali- ja terveydenhuollon erityislakeja. Keskeisiä henkilötietojen käsittelyyn liittyviä säädöksiä ovat 25.5.2018 voimaan astunut EU:n yleinen tietosuoja-asetus (GDPR) sekä kansallinen tietosuojalaki (1050/2018). Sosiaali- ja terveystietojen toissijaisesta käytöstä on säädetty nk. toisiolaissa (552/2019) sekä laissa julkisen hallinnon tiedonhallinnasta (906/2019).

Palvelutuotannon aikana ja sen päätyttyä sivulliselle ei saa ilmaista palvelutuotannon vuoksi tietoon saatuja Päijät-Hämeen hyvinvointialueen tai sen potilaita ja asiakkaita, sopimusumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä ja luottamuksellisia tietoja. Tällaisia ovat myös liike- ja ammattisalaisuudet sekä arkaluontoiset henkilötiedot, ellei julkisuuslainsäädännössä toisin määrätä.

Salassapito koskee myös harjoittelijoita tai muotoon henkilöitä, jotka toimivat terveyden- tai sosiaalihuollon tai pelastustoimen järjestäjän tai tuottajan toimeksiannosta tai sen lukuun.

Palvelutuotannon osalta sovitaan aina kulloinkin kirjallisesti niistä tietojärjestelmistä, pilvipalveluista, tietoteknisistä tai tietotekniikkaa hyödyntävistä lääkintä- tai muista laitteista (kyberturvallisuus huomioon ottaminen), arkkitehtuuriratkaisuista, rekistereistä, käytännön tietoteknisistä toimintatavoista ja työruutiineista sekä tiedon (rekisterien) arkistointi-, luovuttamis- ja hävittämismenettelyistä, joita kyseiseen palvelutuotantoon kokonaisuudessaan liittyy.

Tarkastelu tulee tehdä kaikkien kyseiseen palvelutuotantoon liittyvien mahdollisten alihankintatoimintojen osalta vähintään siltä osin kuin kyseessä on henkilötietojen tai muiden luottamuksellisten tietojen käsittely. Tarkastelu tulee tehdä ennen palvelutuotannon käynnistymistä. Toimittaja osallistuu Tilaaajan pyynnöstä tietojärjestelmäselosteen laatimiseen.

2. Käyttäjätunnukset hyvinvointialueen tietoverkkoihin, tietojärjestelmiin, tietokantoihin ja muihin resursseihin

Palveluntuottajan toiminnassaan tarvitsemat käyttäjätunnukset annetaan, muutetaan ja poistetaan aina hyvinvointialueen tietohallinnon tai vastaavan toiminnallisen tahon tai sen valtuuttaman tahon tekemänä.

Palveluntuottajan saamat käyttöoikeudet ovat aina henkilökohtaisia. Mikäli palveluntuottaja tarvitsee tilapäisesti palvelun tuottamiseksi joitain sellaisia erillisiä tietotekniseen operointiin tai muuhun vastaavaan toimintaan liittyviä tunnuksia, jotka ovat ainoastaan tietohallinnon tai vastaavan toiminnallisen tahon tai sen valtuuttaman tahon joidenkin asiantuntijoiden tiedossa, tulee näissäkin tapauksissa palveluntuottajan edustajan näillä tunnuksilla tekemä käyttö olla jälkikäteen yksilöitävissä ja jäljitettävissä kyseiseen henkilöön. Tällainen toimintatapa on ainoastaan tilapäisesti sallittua, hyvinvointialueen tietohallinto tai vastaavan toiminnallisen tahon tai sen valtuuttama taho vastaa siitä, että tunnukset annetaan käyttöön ja poistetaan käytöstä asianmukaisesti.

Hyvinvointialueen tietoverkon ulkopuolisten etäyhteyksien osalta toimitaan hyvinvointialueen tietohallinnon tai vastaavan toiminnallisen tahon määrittelemillä tietoturvallisilla toimintatavoilla niin, että tällaisia etäyhteyksiä käytetään pääasiassa ainoastaan rajatusti ja tilapäisesti jonkin asian välittömään hoitamiseen. Etäyhteydet on aina välittömästi purettava, kun edellä mainittua tilapäistä tarvetta ei enää ole.

3. Laitteiden ja ohjelmistojen asentaminen, käyttö ja kyberturvallisuus

Hyvinvointialueen sisäisiin tietoverkkoihin ei lähtökohtaisesti saa liittää palveluntuottajan omia laitteita ja ohjelmistoja. Mikäli jonkin hyvinvointialueelle hankitun ohjelmiston, laitteen tai muun vastaavan asentamiseksi on aivan välttämätöntä käyttää toimittajan omia ratkaisuja ja työkaluja, tulee tämä tehdä hyvinvointialueen tietohallinnon tai vastaavan toiminnallisen tahon tai sen valtuuttaman tahon välittömässä valvonnassa tietoturvallisuutta vaarantamatta. Tällöinkin tulee menetellä siten, että kaikki asentamisen kannalta tarpeeton otetaan pois käytöstä tai käyttö estetään. Asennuksien jälkeen on edelleen varmistettava tietoturvallisuuden vaarantamattomuudesta ennen asennettujen palveluiden ottamista käyttöön hyvinvointialueen tietoteknisessä infrastruktuurissa.

Tietojärjestelmiä, ohjelmistoja ja hyvinvointialueen tietoverkkoja tulee käyttää annettujen käyttö- sekä tietoturvallisuus-ohjeiden mukaisesti.

Lääkintä- ja rakennusteknisten sekä muiden laitteiden kyberturvallisuuteen liittyvät määräykset, asennus- ja

käyttöohjeet tulee varmistaa hyvinvointialueen tietohallinnon tai vastaavan toiminnallisen tahon tai sen valtuuttaman tahon asiantuntijoiden kanssa.

4. Seuraamukset tietoturvallisuuden vaarantamisesta ja potilas- ja asiakastietojen väärinkäytöksistä

Potilas- tai asiakastietojärjestelmien tietojen lainvastainen käsittely voi esimerkiksi täyttää jonkin seuraavan rikoksen tunnusmerkistön:

- henkilökisteririkos (RL 38:9 §)
- henkilötietojen käsittelyn rikkominen tai laiminlyönti (tietosuoja-laki luku 4)
- salassapitovelvollisuuden rikkominen (RL 38:1 ja 2 §)
- virkasalaisuuden rikkominen ja tuottamuksellinen virkasalaisuuden rikkominen (RL 40:5 §)
- sähköisestä lääkemääräyksestä annetun lain rikkominen (26 §, tietomurto, RL 38:8 §)

Jos kyseessä on vakava lainvastaisuus, väärinkäytöksestä tehdään aina tutkintapyyntö poliisille. Rikostutkinta on myös ainoa keino siinä tilanteessa, että väärinkäytöksestä epäiltyyn henkilöön ja hänen edustamaansa palveluntuottajaorganisaatioon ei ole voimassa olevaa sopimusta, jolloin ei voida enää käyttää sopimuksessa sovittuja seuraamuksia.

5. Sopimusrikkomukset ja vahingonkorvausvastuu

Tietosuoja koskevien säännösten rikkomisesta voi olla seurauksena myös vahingonkorvauslain mukainen vahingonkorvausvelvollisuus.

Palveluntuottajaorganisaation mahdollisista vahingonkorvausvastuista tässä yhteydessä tarkastellaan palveluntuotannosta tehtyjen sopimusten puitteissa.

Lisäksi EU:n tietosuoja-asetuksessa ja kansallisessa tietosuolaissa säädetään mahdollisista oikeuksista korvaukseen ja sanktioista.

Olemme perehtyneet yllä oleviin palvelutuotantoon liittyviin hyvinvointialueen tietoturva-, tietosuoja- ja kyberturvallisuusperiaatteisiin, ohjeisiin sekä käytänteisiin ja sitoudumme palveluntuottajaorganisaationa noudattamaan niitä siltä osin, kun ne koskevat sopimuksen mukaista palvelua. Palveluntuottajana vastaamme siitä, että työntekijämme toimivat tässä sitoumuksessa edellytetyllä tavalla. Lisäksi vastaamme ja huolehdimme siitä, että käyttämämme mahdolliset alihankkijat työntekijöineen noudattavat samoja

tässä palvelutuotannon tietoturvaluussitoumuksessa esitettyjä hyvinvointialueen digitaaliseen turvallisuuteen liittyviä periaatteita ja sääntöjä.

Palvelutuotannon tietoturvaluussitoumus voidaan allekirjoittaa erikseen tälle sivulle tai todentaa allekirjoitukset sopimuksen ja sen liitteiden yhteydessä, jolloin erillisiä allekirjoituksia ei nimenomaisesti tarvita alla oleviin kohtiin. Mikäli palvelutuotantoon liittyy henkilötietojen käsittelyä, niin **tämän sitoumuksen allekirjoituksella sitoudutaan Henkilötietojen käsittelyn ehtoihin ja Selosteeseen käsittelytoimista.**

Paikka ja päiväys

Palveluntuottajaorganisaation nimi ja Y-tunnus

Yhteyshenkilön nimi, asema¹ tai ammattinimike

Allekirjoitus sekä nimen **selvennys**

¹ Henkilö, jolla on kyseiseen palvelutuotantoon liittyvien sopimusten nimenkirjoitusoikeus