Tietoturvapäällikkö

PHSOTEY versiot 1-3 (11.11.2013, 30.9.2014, 7.10.2015)
PHHYKY – 2. versio 10.4.2018 (1. versio 29.8.2017)
PHHYKY – 3. versio 24.6.2019
PHHYKY – 4. versio 1.10.2019

PALVELUTUOTANNON TIETOTURVALLISUUSSITOUMUS

Jos jokin alla mainittu kohta tai sen asiasisältö ei liity tarjottuun palveluun, kyseistä kohtaa ei tällöin sovelleta palvelutuotannon toteuttamisessa eikä siihen voida vedota mahdollisissa ristiriitatilanteissa.

1. Salassapito palvelutuotannossa digitaalisen turvallisuuden varmistamiseksi

- Salassapitovelvollisuudesta (**asiakirjasalaisuus** ja **vaitiolovelvollisuus**) säädetään yleislaeissa sekä sosiaali- ja terveyshuollon erityislaeissa. **Potilas- ja asiakastiedot ovat terveyden- ja sosiaalihuollon erityislainsäädännön mukaisesti salassa pidettäviä**. Tässä sitoumuksessa ei ole erikseen lueteltu kaikkia yleislakeja eikä 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). Toisiolain tavoitteena on mahdollistaa sosiaali- ja terveydenhuollon toiminnassa sekä sosiaali- ja terveysalan ohjaus-, valvonta-, tutkimus- ja tilastotarkoituksessa tallennettujen henkilötietojen tehokas ja tietoturvallinen käsittely. Lisäksi toisiolain tavoitteena on turvata yksilön luottamuksensuoja sekä oikeudet ja vapaudet henkilötietoja käsiteltäessä.

- Palvelutuotannon aikana ja sen päätyttyä sivulliselle ei saa ilmaista palvelutuotannon vuoksi tietoon saatuja Päijät-Hämeen hyvinvointikuntayhtymän tai sen potilaita ja asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja. Tällaisia ovat myös liike- ja ammattisalaisuudet sekä arkaluontoiset henkilötiedot, ellei julkisuuslainsäädännössä toisin määrätä. **Salassapito koskee myös harjoittelijoita tai muutoin henkilöitä, jotka toimivat terveyden- tai sosiaalihuollon järjestäjän tai tuottajan toimeksiannosta tai sen lukuun.**

- Palveluntuotannon 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 työrutiineista 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 Tilaajan pyynnöstä tietojärjestelmäselosteen laatimiseen.

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

- Palveluntuottajan toiminnassaan tarvitsemat käyttäjätunnukset annetaan ja poistetaan aina kuntayhtymän tietohallinnon tai vastaavan toiminnallisen tahon tai sen valtuuttaman tahon tekemänä.

- Palveluntuottajan saamat käyttäjätunnukset 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 toimintapa on ainoastaan tilapäisesti sallittua, kuntayhtymän tietohallinto tai vastaavan toiminnallisen tahon tai sen valtuuttama taho vastaa siitä, että tunnukset annetaan käyttöön ja poistetaan käytöstä asianmukaisesti.

- Kuntayhtymän tietoverkon ulkopuolisten etäyhteyksien osalta toimitaan kuntayhtymän 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

- Yhtymän sisäisiin tietoverkkoihin ei lähtökohtaisesti saa liittää palveluntuottajan omia laitteita ja ohjelmistoja. Mikäli jonkin yhtymälle hankitun ohjelmiston, laitteen tai muun vastaavan asentamiseksi on aivan välttämätöntä käyttää toimittajan omia ratkaisuja ja työkaluja, tulee tämä tehdä kuntayhtymän 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 kuntayhtymän tietoteknisessä infrastruktuurissa.

- Tietojärjestelmiä, ohjelmistoja ja yhtymän tietoverkkoja tulee käyttää annettujen käyttö- sekä tietoturvallisuusohjeiden mukaisesti.

- Lääkintä- ja rakennusteknisten sekä muiden laitteiden kyberturvallisuuteen liittyvät määritykset, asennus- ja käyttöohjeet tulee varmistaa kuntayhtymän 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:
  - henkilörekisteririkos (RL 38:9 §)
  - henkilötietojen käsittelyn rikkomus tai laiminlyönti (tietosuojalaki 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

- Tietosuojaa 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 tietosuojalaissa säädetään mahdollisista oikeuksista korvaukseen ja sanktioista.

Olemme perehtyneet yllä oleviin palvelutuotantoon liittyviin kuntayhtymän tietoturva-, tietosuoja- ja kyberturvallisuusperiaatteisiin, ohjeisiin sekä käytänteisiin ja sitoudumme palveluntuottajaorganisaationa noudattamaan niitä. Palveluntuottajana vastaamme siitä, että työntekijämme toimivat tässä sitoumuksessa edellytetyllä tavalla. Lisäksi vastaamme ja huolehdimme siitä, että käyttämämme mahdolliset alihankkijat työntekijöineen noudattavat samoja tässä palvelutuotannon tietoturvallisuussitoumuksessa esitettyjä kuntayhtymän digitaaliseen turvallisuuteen liittyviä periaatteita ja sääntöjä. Palvelutuotannon tietoturvallisuussitoumus 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 myös GDPR-liitteiden ehtoihin.**

Paikka ja päiväys _____

Palveluntuottajaorganisaation nimi ja Y-tunnus _____

_____

Yhteyshenkilön nimi, asema[1] tai ammattinimike _____

_____

Allekirjoitus sekä nimen **selvennys** _____

[1] Henkilö, jolla on kyseiseen palvelutuotantoon liittyvien sopimusten nimenkirjoitusoikeus.