13.12.2020

Sosiaali- ja terveysvaliokunta
HE 212/2020

Lausuntopyyntö: Sosiaali- ja terveysvaliokunta perjantai 04.12.2020 klo 09.00 / HE 212/2020 vp / Asiantuntijapyyntö

F-Secure näkee kyberturvallisuuden nykyisessä verkostoituneessa toimintaympäristössä vaativan tiedonkäsittelijöiltä yhdenmukaisen kontrollirakenteen käyttämistä läpi tiedon elinkaaren. Hallituksen esitys luo pohjan toimijoiden väliseen luottamukseen ja selkeyttää tiedonkäsittelyn kontrollien yhteneväisyyttä.

Hallituksen esitys on laadittu kattamaan laajasti sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä ja haluamme tuoda esiin seuraavat asiat, jotka tulisi huomioida lainvalmistellussa.

Yleisesti esityksen sisällöstä

Tiedonkäsittelyn tietoturvallisuuden osalta merkittävät toimijat ovat:

Ohjelmiston valmistaja, joka vastaa ohjelmiston laadusta ja sen osana tietoturvallisesta kehittämisestä. Ohjelmistoon luodaan kyvykkyys tiedon käytön valvonnalle ja turvallisuuskontrolleille.

Tietojärjestelmän valmistaja, joka yhdistelee ohjelmistoja tietojärjestelmäksi ja vastaa ohjelmistojen välisestä integraation ja lisäpalveluiden toteutuksesta.

Tietojärjestelmäpalvelun tuottaja, tarjoaa ja toteuttaa tiedonkäsittely-ympäristön, jossa tietojärjestelmä varsinaisesti tuotetaan, valvotaan ja hallinnoidaan. Tietojärjestelmäpalvelun tuottaja vastaa myös tietojärjestelmän käyttäjätuen. Tietojärjestelmä voidaan tuottaa jaetulta alustalta (SaaS palveluna) tai hyödyntäjälle yksilöitynä erillispalveluna.

Tietojärjestelmän hyödyntäjä, jonka sosiaali- ja terveyspalvelun tai sen osan tuottamiseen käytetään tietojärjestelmää. Hyödyntäjä vastaa tiedon käsittelyn tietoturvallisuudesta päätelaitteiden, käyttöpaikkojen ja henkilöstön osalta. Hyödyntäjällä voi olla useita tietojärjestelmiä ja kumppaneita, joiden integraatiovastuu on hyödyntäjällä tai tämän osoittamalla kokonaisvastuullisella palvelun tuottajalla.

F-Secure Corporation Tammasaarenkatu 7 P.O. Box 24 FI-00181 Helsinki Finland
Tel: +358 9 2520 0700 www.f-secure.com
Business id 0705579-2 Registered office Helsinki

13.12.2020

Sosiaali- ja terveysvaliokunta
HE 212/2020

Hallituksen esityksessä käytetään tiedonsaantioikeudessa loki-tieto termiä, joka johtaa harhaan. Esityksessä tarkoitetaan ilmeisesti käyttöloki- tietoa, joka osoittaa tiedon käytön.

Hallituksen esitys on voimakkaasti tietojärjestelmäkeskeinen, kun sen tulisi esittää vaatimukset tiedon käsittelyn ja säilytyksen vaatimuksia tiedonkäsittelyjärjestelmälle ja niiden käytölle. Vaatimuksia on mahdollisuus täydentää vastaamaan teknologista kehitystä Terveyden- ja hyvinvointilaitoksen toimesta laadituilla ohjeilla ja täydennyksillä.

8§ Valtakunnalliseen arkistointipalveluun tallennettavat asiakirjat

Valtakunnallisen arkistointipalvelun käyttäminen tulisi osaltaan vähentää palveluyksiköltä vaadittavia säilytysaikoja, jolloin osa tiedon elinkaaresta tapahtuisi arkistointipalvelun puolesta.

13 § Omatietovaranto

Hyvinvointitietojen tallentaminen tulisi sallia vain rekisteröidyistä tietojärjestelmistä, jolloin varmistetaan tiedon eheys ja luotettavuus. Henkilö voi hyväksyä tietojensa siirron rekisteröidystä palvelusta, jossa käyttäjältä lisäksi pyydetään lupa tiedon siirtoon ja sen laajuuteen. Tiedonsiirto tapahtuu tämän jälkeen automaattisesti järjestelmien välillä.

27§ Tietoturvasuunnitelma

Tietoturvasuunnitelmassa tulisi käydä selväksi myös tietojärjestelmäkokonaisuutena sisäisien ja ulkoisien toimijoiden vastuut toteuttaa ja ylläpitää tietoturvakontrolleja, joka ilmaistaan esim. vastuunjakotaulukolla.

Tietoturvasuunnitelman tulee kattaa tietoturvanjohtamisjärjestelmän koko laajuus mukaan lukien haavoittuvuuksienhallintaprosessi, sekä tietoturvan ja riskienhallinnan varmistamisen toimet vuosikellossa.

F-Secure Corporation Tammasaarenkatu 7 P.O. Box 24 FI-00181 Helsinki Finland
Tel: +358 9 2520 0700 www.f-secure.com
Business id 0705579-2 Registered office Helsinki

13.12.2020

Sosiaali- ja terveysvaliokunta
HE 212/2020

33§ Tietojärjestelmäpalvelun tuottajan ja valmistajan sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet

Hyvinvointisovelluksen valmistaja tuottaa ohjelman, jonka käyttäjä asentaa ja ottaa käyttöön omassa hallinnassaan olevassa laitteessa. Sovelluksen kerätessä käyttäjän tiedot käyttäjän hallussa olevaan laitteeseen, ei vielä muodosta varsinaista tietojärjestelmää, mutta kun tiedot siirtyvät taustajärjestelmään, niin se tulisi käsittää vastaavasti tietojärjestelmäpalveluksi, kuin laissa on termiä käytetty.

37 § Tietoturvallisuuden arviointi

Sertifiointi edellyttää sertifiointiohjelman toteuttamista, jolla määritellään ja ylläpidetään kriteeristö, jota vasten auditointi suoritetaan. Kriteeristön pohjan luo esitetty laki, johon Terveyden- ja hyvinvointilaitokselle annetaan oikeus laatia tarkennuksia. Hallituksen esityksessä auditoinnin tekijäksi on osoitettu arviointilaitos, joka tuo luotettavan ja yhtenevän tarkastuksen eri toimijoille ja tietojärjestelmissä käytetyille teknologioille. Sertifioinnille laissa määritetään 3 vuoden enimmäisvoimassaoloaika, jonka puitteissa toimija toteuttaa tietoturvasuunnitelman mukaisia toimia ja valvoo sitä omavalvonnan keinoin huomattavasti tiiviimmässä syklissä.

Auditointi todentaa tietyn ajanhetken osalta kontrollien kattavuuden ja tehokkuuden, sekä arvioi kohteen kyvykkyyden ylläpitää tavoiteltua tietoturvan tasoa toiminnassaan. Tämän tukemiseksi omavalvontaa tulee tehostaa säännöllisellä ja objektiivisella tarkastuksilla sertifiointi kaaren sisällä, joka noudattaa laadittua tietoturvasuunnitelmaa.

Toimittajalla tulisi myös olla mahdollisuus hyödyntää ISO27001 sertifioitua johtamisjärjestelmää osana tarkastusvastuuta.

Helsingissä 03.12.2020

Pasi Korhonen
Johtava tietoturvakonsultti
F-Secure Corporation
pasi.korhonen@f-secure.com
+358 40 591 6497