Vastaus kirjalliseen kysymykseen KKV 801/2020 vp

Vastaus kirjalliseen kysymykseen sosiaali- ja terveydenhuollon tietoturvallisuudesta ja kyberturvallisuudesta

Eduskunnan puhemiehelle

Eduskunnan työjärjestyksen 27 §:ssä mainitussa tarkoituksessa Te, Arvoisa puhemies, olette toimittanut asianomaisen ministerin vastattavaksi kansanedustaja Mia Laihon /kok näin kuuluvan kirjallisen kysymyksen KK 801/2020 vp:

Miten valvotaan Kanta-palveluiden ulkopuolella olevien yritysten tietohallintopalveluita, niiden asiakastiedon ja tietoturvan hallintaa ja tasoa,

miten hallitus varmistaa, ettei laajoissa kansalaisten tietoja sisältävissä järjestelmissä kuten Kanta-palveluissa ole tietoturvariskejä,

onko hallitus tehnyt riskinarviota ja riskinhallintasuunnitelmaa sote-maakuntaratkaisuun liittyen tietojärjestelmien osalta,

miten hallitus on huomioinut sote-lakivalmistelussa tietojärjestelmien tietoturva-asiat,

kuinka hallitus on arvioinut riittävän tietoturvan sote-palveluissa käytettäviin digitaalisiin palveluihin, potilastietojärjestelmiin ja henkilöstöhallintoon,

miten henkilöstöhallinnon tietoturva on huomioitu sote-valmistelussa,

miten asiakastietojen luottamuksellisuuden lisäksi huomioidaan henkilökunnan tietoturva,

milloin hallitus on tuomassa eduskuntaan tietojen käsittelyä koskevan kokonaislainsäädännön uudistuksen,

miten hallitus on huomioinut sote-lain valmistelussa asiakastyössä käytettävän digitalisaation korkeatasoisen tietoturvan niin, että kaikki tiedot pysyvät luottamuksellisina ja

kuinka hallitus varmistaa, että robotiikan ja terveydenhuollon digitalisaation kyberuhat ja hyökkäykset esim. lääkinnällisten laitteisiin, ohjelmistojen haavoittuvuuteen, mobiililaitteisiin, etähallittaviin laitteisiin ja järjestelmien käyttötapoihin sekä salasanakäytänteisiin huomioidaan nykytilanteessa ja suunnitellussa sote-uudistuksessa?

Vastaus kirjalliseen kysymykseen KKV 801/2020 vp

Vastauksena kysymykseen esitän seuraavaa:

Sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevassa laissa (159/2007, asiakastietolaki) säädetään mm. sosiaali- ja terveydenhuollon palvelunantajien tietoturvaa ja tietosuojaa koskevasta omavalvontasuunnitelmasta, palvelunantajien ja tietojärjestelmän valmistajien vastuista, asiakas- ja potilastietoja käsittelevien tietojärjestelmien tietoturvavaatimuksista sekä valvonnasta. Asiakastietolaissa säädetään myös tietojärjestelmien kuulumisesta A-ja B-luokkiin. A-luokkaa ovat kaikki Kanta-palveluun liitettävät asiakas- ja potilastietojärjestelmät, B-luokkaa ne järjestelmät, joita ei ole tarkoitettu liitettäväksi Kanta-palveluun.

Kanta-palveluihin liitettävät tietojärjestelmät on sertifioitava ennen liittymistä Kanta-palveluun. Monet asiakastietolain mukaisista vaatimuksista koskevat kuitenkin kaikkia asiakas- ja potilastietojärjestelmiä. Esimerkiksi tietojärjestelmiä koskevat olennaiset vaatimukset, tietojärjestelmän valmistajan yleiset velvollisuudet sekä valvonta koskevat yhtä lailla niin A- kuin B-luokan järjestelmiä. Myös palvelunantajan vastuu omavalvontasuunnitelmasta koskee myös Kantaan liittymättömiä palvelunantajia, samoin palvelunantajan vastuu ilmoittaa tietojärjestelmän poikkeamista sosiaali- ja terveysalan lupa- ja valvontavirasto Valviralle. Palvelunantajan on myös seurattava ja valvottava, että sen antamaan palveluun liittyvä tietosuoja ja tietoturva toteutuvat.

Valvonnan osalta asiakastietolaissa säädetään palvelunantajan valvontavastuusta. Valviran valvontavastuu koskee sekä A- että B-luokan järjestelmiä, ja molempiin luokkiin kuuluvat järjestelmät on ilmoitettava Valviran tietojärjestelmärekisteriin. Samoin valvonnan keinot ovat samat kaikille tietojärjestelmille, esim. määräys tuotantokäytössä olevan järjestelmän puutteiden korjaamisesta, tietojärjestelmän käytön kieltäminen ja uhkasakko. Valvontaviranomaisen toteuttaman valvonnan laajuudesta riippumatta keskeistä on kuitenkin edelleen kunkin palvelunantajan vastuu tietoturvan toteutumisesta omassa toiminnassaan ja järjestelmissään.

EU:n yleisen tietosuoja-asetuksen mukaan tietosuojavaltuutettu valvoo asetuksen ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista. Tietosuojavaltuutetun tehtävistä ja valtuuksista säädetään tietosuoja-asetuksessa (55-59 art). Lisäksi tietosuojalaki (1050/2018) täydentää asetusta, ja laissa säädetään esimerkiksi hallinnollisen seuraamusmaksun määräämisestä, jos tietosuoja-asetusta on rikottu. Tietosuojavaltuutetulla on käytössään myös muita toimenpiteitä, kuten varoitus, huomautus ja käsittelyä koskevien rajoitusten asettaminen.

Hallitus on antanut eduskunnalle asiakastietolakia koskevan muutosesityksen (HE 212/2020 vp). Siinä esitetään liittymisvelvoitetta Kanta-palveluihin kaikille sosiaali- ja terveydenhuollon toimijoille, joilla on käytössään potilas- tai asiakastietojärjestelmä. Tämä tarkoittaa sitä, että suuri joukko nyt sertifioinnin ulkopuolelle jääneitä B-luokan järjestelmiä siirtyy A-luokkaan ja niille on tehtävä ulkopuolisen tahon suorittama sertifiointi.

Siltä osin kuin asiakas- ja potilastietoihin sisältyy henkilökuntaa koskevia tietoja (esimerkiksi nimi ja yksilöintitunnisteet), koskevat asiakastietolain säädökset ja tietoturvallisuusvaatimukset myös niitä. Jos henkilökunnan henkilötietoja käsitellään palvelunantajan muissa järjestelmissä, on palvelunantajan noudatettava muun lainsäädännön mukaisia, henkilötietojen käsittelyä koskevia vaatimuksia kuten EU:n yleinen tietosuoja-asetus ja tietosuojalaki.

Vastaus kirjalliseen kysymykseen KKV 801/2020 vp

Kanta-palveluiden toteutus on asiakastietolaissa säädetty Kelan tehtäväksi, ja Kela vastaa Kanta-palveluiden lainmukaisesti toteuttamisesta ja niiden tietoturvallisuudesta. Kanta-palvelujen tiedot on suojattu monin tavoin sekä tietoverkkojen, tietokantojen että sovellusten osalta, ja Kanta-palvelut on sertifioitu ulkopuolisen tietoturvallisuuden arviointilaitoksen toimesta. Vaikka tietojärjestelmät on tehty mahdollisimman turvallisiksi, Kelan on kehitettävä Kanta-palveluiden tietoturvaa jatkuvasti kyberuhkiin varautumiseksi.

Tiedonhallintasäädösten kokonaisuudistuksen käynnistämistä on valmisteltu sosiaali- ja terveysministeriössä. Uudistusta on tarkoitus vaiheistaa. Tavoitteena on, että ensimmäisen vaiheen HE annettaisiin Eduskunnalle tämän hallituskauden aikana. Kokonaisuudistuksen keskeisiä sisältöjä ovat tietosuojasäädösten selkiyttäminen ja yhtenäistäminen sekä laintasoinen sääntely potilasasiakirjoista ja toimintansa päättäneiden yksityisten palveluntuottajien asiakirjojen säilyttämisestä.

Sote-uudistuksessa palveluiden järjestämisvastuu siirtyy kunnilta uusille toimijoille ja palveluiden tuotannon organisointi muuttuu. Siten esimerkiksi kaikki digitaaliseen turvallisuuteen liittyvät velvollisuudet säilyvät ennallaan uudessa organisaatiossa. Tämä koskee asiakas- ja potilastietoja, henkilöstöhallinnon tietoja sekä tuotettavien palveluiden turvallisuutta. Näistä on säädetty mm. terveydenhuoltolaissa, asiakastietolaissa, julkisuuslaissa, tiedonhallintalaissa sekä henkilötietolaissa. Uusien toimijoiden on täytettävä tietosuojaan ja -turvallisuuteen liittyvät vaatimukset jatkossakin.

Lainsäädännöllisesti palveluiden tuottaja on vastuussa tuottamistaan palveluista niiden toteutustavasta riippumatta. Sosiaali- ja terveyspalveluiden tuottaja on vastuussa siitä, että arkaluontoiset asiakas- ja potilastiedot eivät paljastu sivullisille ja tämä vaatimus on täytettävä myös digitaalisissa palveluissa.

Terveydenhuollossa käytettävät sähköiset palvelut ovat ajanvaraus- ja laskutuspalveluita lukuun ottamatta pääsääntöisesti lääkinnällisiä laitteita, joiden on täytettävä lääkinnällisiä laitteita koskevat vaatimukset. Lääkinnällisten laitteiden vaatimusmäärittelyihin on valmisteilla turvallisuutta koskeva osio, jonka avulla parannetaan niiden kyberturvallisuutta.

Helsingissä 17.11.2020

Perhe- ja peruspalveluministeri Krista Kiuru