Heli Geitlin

30.9.2020

Toiminnanjohtaja Lea Suoninen-Erhiö
Huoltajasäätiö sr
Lea.Suoninen-Erhio@huoltaja-saatio.fi

Viite: Huoltaja-säätiön sosiaalihuollon asiantuntijaryhmän etätyön ja –palveluiden tietoturvaa koskeva kannanottopyyntö

KANNANOTTOPYYNTÖ: ”DIGILOIKKA TIETOTURVALLISESTI ”

Huoltaja-säätiön yhteydessä toimiva sosiaalihuollon asiantuntijaryhmä (jäljempänä asiantuntijaryhmä) on jättänyt sosiaali- ja terveysministeriölle (STM) 12.6.2020 kannanottonsa ”Digiloikka tietoturvallisesti” (jäljempänä kannanotto). STM siirsi asian Terveyden ja hyvinvoinnin laitoksen (THL) vastattavaksi 23.6.2020. Asiantuntijaryhmä toteaa kannanotossaan, että sosiaalihuollossa digitalisaatio ja etätöihin siirtyminen etenivät kevään 2020 aikana nopeasti. Kannanoton mukaan sosiaalihuollon etätyöhön ja etäpalveluihin liittyviin tietosuoja- ja tietoturvakysymyksiin tulisi luoda kansallisia linjauksia ja ohjeistuksia sekä huolehtia työntekijöiden kouluttamisesta yhdenmukaisesti koko maassa.

Huolimatta poikkeusoloista ja laajamittaisesta etätyöhön siirtymisestä, sosiaali- ja terveydenhuollon organisaatioiden on pitänyt edelleen kyetä toimimaan. Sosiaalihuollon tehtävänä on tukea haavoittuvassa asemassa olevia henkilöitä sekä turvata välttämätön hoiva, huolenpito ja toimeentulo. Tämä tehtävä korostuu entisestään normaaliolojen häiriötilanteissa ja poikkeusoloissa.

Tietoturvaan ja tietosuojaan liittyvä keskeinen lainsäädäntö

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista siten, että tiedot ovat niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Henkilötietojen käsittelyssä on noudatettava EU:n yleistä tietosuoja-asetusta (2016/679). Tietosuoja-asetuksen 32 artiklassa säädetään käsittelyn turvallisuudesta. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi. Tietosuojalaki (1050/2018) täydentää tietosuoja-asetusta. Lisäksi henkilötietojen käsittelyyn vaikuttaa kunkin toimialan lainsäädäntö. Sosiaali- ja terveydenhuollon tietojen käsittelyssä ja hallinnassa sovelletaan useita eri lakeja ja asetuksia, joista tässä muutamia esimerkkejä. Potilaslaissa (785/1992) säädetään potilasasiakirjojen käsittelystä ja asiakirjoihin sisältyvien tietojen salassapidosta. Potilasasiakirja-asetusta (298/2009) noudatetaan potilasasiakirjojen laatimisessa sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisessä. Sosiaalihuollon asiakaslaissa (812/2000) säädetään asiakkaan oikeuksista hänen tietojensa käsittelyssä ja salassapidossa. Asiakastietolaissa (157/2009) säädetään julkisten ja

yksityisten sosiaali- ja terveyspalveluiden asiakastietojen sähköisestä käsittelystä ja valtakunnallisista tietojärjestelmäpalveluista. Laissa on säännökset tietojen salassapidosta, luovutuksesta, arkistoinnista ja asiakkaan oikeuksista saada tietoa omista asiakastiedoistaan sekä mm. palvelunantajille säädetty velvoite tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelman laatimisesta. Sosiaalihuollon asiakasasiakirjalaissa (254/2015) säädetään asiakastietojen kirjaamisesta ja siihen liittyvistä velvoitteista sosiaalihuollossa. Lisäksi sähköiseen asiointiin liittyvää sääntelyä on hallinnon yleislaeissa ja tiedonhallintaa yleisesti koskevissa laeissa. Tietoturvaan, tietosuojaan ja sähköiseen asiointiin liittyvää sääntelyä tulee noudattaa myös pandemian aikana.

Etätyön sopivat työtehtävät ja turvallinen etätyöympäristö

Keväällä poikkeusolojen toteamisen yhteydessä hallitus antoi etätyösuosituksen. Kyse oli etätyön suosimisesta, jos työtehtävät sen mahdollistavat. Työnantajan harkinta- ja päätäntävallassa on arvioida, mitä työtehtävät mahdollistavat. Työnantaja päättää työn suorittamisen paikasta tehdyn työsopimuksen mukaisesti. Lähtökohtana on, että työnantaja ja työntekijä sopivat etätyön tekemisestä ja siihen liittyvistä ehdoista ja yksityiskohdista. Etätöihin siirtyminen on muutos aiempaan sopimukseen, joten siitä tulee sopia kuten muista muutoksista. Etätyöjärjestelyä koskeva sopimus on suositeltavaa tehdä kirjallisesti. Etätyössä ja siihen siirtymisessä noudatetaan voimassa olevaa lainsäädäntöä, muun muassa työsopimuslakia (55/2001), kunnallisesta viranhaltijasta annettua lakia (304/2003) ja työsopimusmääräyksiä. Työturvallisuuslain (738/2002) mukaisesti työnantaja vastaa työpaikan turvallisuudesta tilanteessa, jossa työnantaja edellyttää työn suorittamista työpaikalla.

Kaikki sosiaalihuollon työtehtävät eivät sovi tehtäväksi etätyönä. Kaikkea työtä ei myöskään voi tehdä tietoturvallisesti kotona. Nämä työt sekä tietoturvaan ja tietosuojaan liittyvät riskit olisi kyettävä tunnistamaan.

Etätyöskentelyssä kotona tai muussa sovitussa etätyön tekemisen paikassa tulee noudattaa tietosuojaan ja tietoturvaan liittyvää sääntelyä ja ohjeita. Työtilan tulee olla työtehtävien vaatimalla tasolla ja täyttää tietoturvallisuuden asettamat vaatimukset. Työntekijän tulee toimia huolellisesti ja vastuullisesti, tietosuojaan ja -turvaan liittyviä ohjeita noudattaen. Lähtökohtana yleensä on, että työntekijän tulee käyttää työnantajan tarjoamia laitteita ja yhteyksiä. Laitteita ei saa antaa muiden käyttöön ja laite tulee pitää lukittuna silloin kun sitä ei käytetä.

Sosiaali- ja terveydenhuollossa käsitellään salassa pidettäviä asiakas- ja potilastietoja. Jo pelkästään se tieto, että henkilö on sosiaali- tai terveydenhuollon asiakas, on salassa pidettävä tieto, jota ei saa ilmaista sivullisille. Sivullisella tarkoitetaan sellaista henkilöä, jolla ei ole lainmukaista oikeutta tiedon saantiin. Myös perheenjäsen on sivullinen.

Etäpalvelujen antajan on täytettävä muun muassa asiakastietolaissa asetetut vaatimukset. Etäpalvelujen antajan on laadittava tai päivitettävä Terveyden ja hyvinvoinnin laitoksen määräyksen (2/2015)[1] mukainen omavalvontasuunnitelma etäpalvelujen sisältö huomioiden. Palvelunantajan tulisi suunnitella myös etätyön näkökulmasta THL:n omavalvontasuunnitelmaa koskevan määräyksen mallipohjan kohdan 4 mukaisesti käyttöympäristön tietoturvakäytännöt, eli muun muassa tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus. Käytännössä tämä tarkoittaa esimerkiksi tilojen lukitsemisesta, näyttöpäätteiden suojaamisesta, virusturvasta ja

[1] https://thl.fi/documents/920442/2816495/Allekirjoitettu_THL_Maarays_2_Omavalvontasuunnitelma_20150130.pdf/2f0f73aa-7299-47d0-be7a-b6c71a36d97e

käyttäjätunnuksista huolehtimista. Häiriötilanteissa ja poikkeusoloissa etätyöskentely saattaa olennaisesti lisääntyä. Kunnan sosiaalihuollosta vastaavan viranomaisen tulee myös tältä osin etukäteen valmiussuunnitelmin varmistaa tehtäviensä mahdollisimman hyvä hoito.

Huoltovarmuuskeskus on julkaissut "Ohjeita turvallisten etätyövälineiden valintaan[2]". Ohje auttaa organisaatioita valitsemaan oikeanlaiset ja turvalliset työvälineet etätyöskentelyyn. Ohjeesta löytyy kuvaus ja käyttösuositus muun muassa WhatsApp-, Zoom- ja Microsoft Teams-sovellusten osalta. Esimerkiksi WhatsAppin osalta todetaan, että kyseessä on "Facebookin omistama alustariippumaton pikaviestintä- ja puhelusovellus. Sovellusta voidaan käyttää julkisen tiedon käsittelyyn ja viestintään, mikäli tiedon luottamuksellisuuden vaarantumisesta ei aiheudu vakavia vaikutuksia." Kyberturvallisuuskeskus on julkaissut ohjeita[3] videoneuvotteluratkaisun valitsemiseen käyttötarpeen ja luottamuksellisuuden mukaan. Edellä mainittujen ohjeiden osalta on otettava huomioon, että ohjeet ovat yleisiä eikä niitä ole annettu erityisesti sosiaali- ja terveydenhuollon palveluiden tai lainsäädännön näkökulmasta.

Organisaation riskiarviopohjainen päätös

Kun sosiaali- ja terveydenhuollossa otetaan käyttöön uusia viestintäratkaisuja, organisaation tulee noudattaa tietosuojasääntelyä. Viestintäratkaisujen valitsemisessa on kiinnitettävä erityisesti huomiota tietosuojaan ja tietoturvaan, jotta voidaan estää henkilötietojen joutuminen sivullisille.[4] Uusia henkilötietojen käsittelytapoja suunniteltaessa, käyttöönotettaessa ja käytettäessä tulee huomioida esimerkiksi salassapitoa, tietosuojaa ja tietoturvaa sekä asiakirjamerkintöjen laatimista koskevat vaatimukset samalla tavalla kuin perinteisesti toteutetuissa lähipalveluissa. Näiden vaatimusten toteuttamisesta ei voi poiketa edes asiakkaan pyynnöstä tai suostumuksella.

Tietosuoja-asetuksen 32 artikla edellyttää, että rekisterinpitäjä ja henkilötietojen käsittelijä toteuttaa sellaiset tekniset ja organisatoriset tietoturvallisuuden varmistamiseen tähtäävät toimenpiteet, jotka vastaavat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä. Riskiarvio on tehtävä rekisteröidyn näkökulmasta eli rekisterinpitäjän on arvioitava mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja mitä vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Rekisterinpitäjän tulee lisäksi arvioida, pitääkö uuden välineen käyttöönotosta tehdä tietosuoja-asetuksen 35 artiklan mukainen vaikutustenarviointi. Vaikutustenarviointi on tehtävä ennen uusien menettelytapojen käyttöön ottamista. Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun suunniteltu käsittely aiheuttaa yksilöiden oikeuksiin ja vapauksiin kohdistuvan korkean riskin.[5] Tietosuoja-asetus myös edellyttää, että rekisterinpitäjä pystyy osoittamaan noudattavansa tietosuojalainsäädäntöä. Toteutetut toimenpiteet ja tehdyt ratkaisut on syytä dokumentoida osoitusvelvollisuuden toteuttamiseksi.[6]

---

[2] https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/07/03140734/Ohjeita-turvallisten-et%C3%A4ty%C3%B6v%C3%A4lineiden-valintaan.pdf
[3] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/valitse-videoneuvotteluratkaisu-kayttotarpeen-ja-tiedon-luottamuksellisuuden-mukaan
[4] https://tietosuoja.fi/koronavirus, Voiko terveydenhuollossa ottaa käyttöön uusia viestintävälineitä pandemian ajaksi?
[5] Lisätietoja riskien arvioimisesta ja vaikutustenarvioinnin laatimisesta on tietosuojavaltuutetun sivuilla, https://tietosuoja.fi/arvioi-riskit ja https://tietosuoja.fi/vaikutustenarviointi
[6] https://tietosuoja.fi/osoitusvelvollisuus

Lähtökohtana on se, että kukin sosiaali- ja terveydenhuollon organisaatio tekee päätöksensä uusien viestintäratkaisujen käyttöönottamisesta riskiarviopohjaisesti. Riskiarviossa rekisterinpitäjän on otettava huomioon muun muassa kyseessä olevien henkilötietojen käsittelyn luonne, laajuus, tarkoitus ja asiayhteys. Asiakas- ja potilastiedot ovat salassa pidettäviä, mikä vaikuttaa riskiarvioon. Arvioitaessa sitä, voidaanko tiettyä viestintäratkaisua käyttää, tulee tarkemmin selvittää muun muassa se, millaisia tietoja sovelluksessa tultaisiin käsittelemään, miten tiedot on suojattu ja millaiset käyttöehdot ko. sovelluksessa on. On myös otettava huomioon, että joissain palveluissa tiedot siirretään EU:n ulkopuolelle. Arvioitavaksi nousee täten myös sääntely liittyen tietojen siirtämiseen EU/ETA-maiden ulkopuolelle. Tietosuoja-asetuksen mukaan rekisteröidyille tulisi kyetä kertomaan mihin kaikkialle tiedot päätyvät, mikä ei välttämättä ole käytännössä mahdollista. Tietojen poistaminen palvelusta ei myöskään välttämättä ole mahdollista.

Terveydenhuollon etäpalveluiden toteuttamisesta on annettu ohjeita ja linjauksia. STM on muun muassa linjannut, että terveydenhuollon etäpalvelut rinnastetaan perinteisiin vastaanottokäynteihin.[7] Valviran terveydenhuollon etäpalveluita koskevan ohjeen[8] mukaan etäpalveluissa tietojen välitykseen ja tallentamiseen käytettävien tietojärjestelmien on täytettävä salassapitoa, tietosuojaa sekä tietoturvaa koskevien säännösten vaatimukset. Vastuu tietosuojasta ja tietoturvallisuudesta niin etäpalveluissa käytettävien yhteyksien kuin siinä syntyvien henkilötietojen käsittelyn osalta on palvelujen antajalla. Sosiaali- ja terveydenhuollossa palveluntuottaja näin ollen vastaa sähköisten viestintäratkaisujen käytännön toteutustavoista. Tällöin tulee arvioida viestintäratkaisujen käyttämiseen liittyvät riskit ja toteutustapa siten, että ne täyttävät samat vaatimukset kuin perinteisissä palveluissa. Sähköisten välineiden käyttämisessä tulee lähtökohtaisesti noudattaa samoja sääntöjä ja periaatteita kuin vastaavan lähipalvelun toteuttamisessa.

THL on julkaissut viranomaisyhteistyössä valmistellun ohjeen yleiseen käyttöön tarkoitettujen ohjelmistojen hyödyntämisestä sote-palveluissa (Ohje 2/2017[9]). Yhtenä ohjeen lähtökohdista ovat olleet myös etäyhteyksiin ja etäpalveluihin käytettävät video-, chat- ja muut vastaavat ohjelmistot. Ohjeen mukaan yleiseen käyttöön tarkoitettuja ohjelmistoja ovat esimerkiksi videoneuvottelu- ja etäpuheluohjelmistot sekä yleiset viestinvälitysohjelmistot. Yleiskäyttöisiä ohjelmistoja on mahdollista hyödyntää sosiaali- ja terveyspalveluja tuottavissa organisaatioissa (käyttäjäorganisaatio) ja eri tyyppisissä palveluissa kuten etävastaanotoilla. Kuten edellä on todettu, sosiaali- ja terveyspalveluja tuottava organisaatio vastaa kuitenkin myös yleiseen käyttöön tarkoitetun ohjelmiston käytöstä vastaavalla tavalla kuin muustakin toiminnassaan tapahtuvasta sosiaali- ja terveyspalveluissa syntyvien tietojen tiedonhallinnasta. Yksityiskohtaisempia tietoturvavaatimuksia ja auditointeja sosiaali- ja terveydenhuollossa edellytetään kansallisesti Kanta-palveluihin liittyviltä A-luokan tietojärjestelmiltä (THL:n määräys 1/2015), jollaisia yleiskäyttöiset ohjelmistot eivät ole. Yleiskäyttöisten ohjelmistojen valmistajat tai käyttäjät voivat myös tukea sosiaali- ja terveydenhuollossa edellytettävien vaatimusten täyttämistä tietosuojan ja tietoturvallisuuden toteuttamiseen tarkoitettujen standardien kautta tai toteuttamalla tietoturvallisuuden ja tietosuojan vaatimusten todentamiseen ulkoisia arviointeja. Valmistaja voi myös kieltää yleiskäyttöisen ohjelmiston käytön esimerkiksi arkaluonteisten asiakas- tai potilastietojen käsittelyyn.

[7] https://stm.fi/-/uusi-linjaus-terveydenhuollon-etapalvelut-rinnastetaan-perinteisiin-vastaanottokaynteihin
[8] https://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/potilaille-annettavat-terveydenhuollon-etapalvelut
[9] https://thl.fi/documents/920442/2902744/ohje_2_2017_Yleiskayttoiset_ohjelmistot.pdf/d96d2f5e-404e-4021-a8ce-ddb0046c9ee7

Julkishallinnon yhteistä tunnistuspalvelua, Suomi.fi-tunnistusta, on suositeltavaa käyttää palveluntuottajan sellaisissa digitaalisissa palveluissa, joissa loppukäyttäjä pitää tunnistaa luotettavasti. Näitä ovat esimerkiksi ns. itsepalvelujärjestelmät, joissa asiakas itse omalla ajallaan suorittaa jonkin toimen ja joka ei vaadi esimerkiksi ammattilaisen osallistumista. Sen sijaan vuorovaikutteisissa etäpalveluissa, joissa asiakas esimerkiksi keskustelee ammattihenkilön kanssa, erilaisia tunnistamistapoja voi hyödyntää laajemmin (esim. asiakas on entuudestaan tuttu, asiakas tunnistetaan äänestä tai kasvoista). Tarkoituksenmukaista ei ole, että vuorovaikutteisissa etäpalveluissa asiakkaan tulisi tunnistautua jokaisella asiointikerralla.

Tietoturvaan liittyviä e-kursseja ja muita hyödynnettäviä materiaaleja

eOppivassa on kaikille avoimia tietoturvaan ja tietosuojaan liittyviä kaikille e-kursseja, joita voi soveltuvin osin hyödyntää omassa organisaatiossa, esimerkiksi:

https://eoppiva.fi/kurssit/toimi_turvallisesti_digimaailmassa/#/lessons/zvEBUoc8i3l1PiowQ5SkyRgV1SdBWdIV

https://www.eoppiva.fi/koulutukset/tietosuojan-abc-julkishallinnon-henkilostolle/

https://www.eoppiva.fi/koulutukset/dataskyddets-abc-for-personalen-inom-den-offentliga-forvaltningen/

https://www.eoppiva.fi/koulutukset/arjen-tietosuoja/

https://www.eoppiva.fi/koulutukset/digiturvallinen-tyoelama/

THL ja Liikenne ja viestintävirasto Traficom ovat yhteistyössä laatineet koonnoksen (liite 1) jo olemassa olevista ja hyödynnettävistä sosiaali- ja terveydenhuollon etäpalveluiden tietosuojaan ja tietoturvaan liittyvistä materiaaleista ja ohjeista. Liitteen lopussa on myös muita aihepiiriin liittyviä linkkejä.

Yhteenveto

Tietosuojaan, tietoturvaan ja sähköiseen asiointiin liittyvää sääntelyä tulee noudattaa myös pandemian aikana ja käytettäessä sähköisiä viestintävälineitä. Sosiaali- ja terveydenhuollon asiakas- ja potilastiedot ovat salassa pidettäviä. Valittavassa välineessä on kiinnitettävä erityistä huomiota tietoturvallisuuteen, jotta tietoja ei päädy sivullisille. Lähtökohtana on se, että kukin sosiaali- ja terveydenhuollon organisaatio tekee päätöksensä uusien viestintäratkaisujen käyttöön ottamisesta riskiarviopohjaisesti. Yleisesti voidaan todeta, että organisaatio vastaa viestintäratkaisujen toteutustavoista ja valittujen ratkaisujen tulee täyttää samat vaatimukset kuin lähipalveluissa.

THL pitää tärkeänä sosiaali- ja terveysministeriön Digitalisaatio terveyden ja hyvinvoinnin tukena Digitalisaatiolinjaukset 2025[10] mukaisesti sitä, että asiakastarpeet ohjaavat kehitystä ja voimavarojen kohdentamista. Palvelut tulee tarjota asiakkaan kannalta mielekkäinä kokonaisuuksina tarveperusteisesti ajasta ja paikasta riippumatta. Hallinnonalan toimintatavat tulee uudistaa tukemaan digitaalisia käytäntöjä. Sähköisten palvelujen on oltava luonnollinen osa palveluketjua. Toimintojen onnistunut asiakaslähtöinen digitalisointi edellyttää, että koko

[10] https://julkaisut.valtioneuvosto.fi/handle/10024/75526

Heli Geitlin 30.9.2020

hallinnonalan digitalisaatiota toteutetaan yhdessä, koordinoidaan ja johdetaan kokonaisuutena. Digitalisaation tukipilareina toimivat tiedot ja tietojärjestelmät laitetaan kuntoon. Linjauksissa myös lähdetään siitä, että digityölle luodaan edellytykset ja yhtenäiset pelisäännöt osana perinteisiä työn tekemisen tapoja.

THL on tämän vastauksen laatimisen yhteydessä käynyt viranomaiskeskustelua sosiaali- ja terveysministeriön kanssa. THL on lisäksi vienyt Vahti-työryhmien tietoon kannanotossa esitetyt kysymykset erityisesti liittyen yleisiin viestintäratkaisuihin. Tietosuojavaltuutetun toimisto on käynyt tämän vastauksen läpi erityisesti tietosuojalainsäädäntöön ja henkilötietojen käsittelyyn liittyvien aihepiirien osalta.

Osalla sosiaali- ja terveydenhuollon organisaatioista on jo käytössä tietoturvallisia viestintäratkaisuja ja organisaatiot ovat myös luoneet hyviä käytäntöjä ja ohjeita henkilökunnalleen ja asiakkailleen. Jo käytössä olevat tietoturvalliset asiointiratkaisut eri hallinnonaloilla tulisi viranomaisyhteistyössä kartoittaa ja niiden soveltuvuus sosiaalihuoltoon arvioida. Kartoituksen perusteella kunnat voisivat ottaa käyttöön tietoturvallisia etäpalveluiden ja -asioinnin muotoja, ja tarjota tämän jälkeen niitä asiakkailleen. Organisaatiot voivat myös omatoimisesti selvittää, millaisia etäpalveluratkaisuja on käytössä tällä hetkellä kuntasektorilla esimerkiksi terveydenhuollossa.

Aleksi Yrttiaho
Tiedonhallintajohtaja

Jarmo Kärki
Yksikönpäällikkö

Liite 1 Sosiaali- ja terveydenhuollon etäpalveluiden tietosuojaan ja tietoturvaan liittyviä ohjeita ja linkkejä