Lakiosasto
Jaana Rissanen

25.1.2019

Eläketurvakeskuksen kommentit hallituksen esityksestä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Eläketurvakeskus katsoo, että lakiesityksen lähtökohtaiset tavoitteet ovat kannatettavia. Lisäksi Eläketurvakeskus toteaa, että esityksessä on huomioitu melko hyvin lausuntokierroksella esiin nostettuja seikkoja.

Eläketurvakeskus haluaisi kuitenkin kiinnittää huomiota eritysesti lakiehdotuksen 4 luvun 14 §:ään ja sen vaikutuksiin Eläketurvakeskuksen ja työeläkealan toiminnassa sekä tietojenvaihtoon eri viranomaisten kanssa. Pykälässä säädetään tietojen siirtämisestä tietoverkossa. Säännöksen mukaan viranomaisen on järjestettävä salassa pidettävän tiedon siirto siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Pykälän yksityiskohtaisissa perusteluissa puolestaan todetaan, että tunnistamista ja varmistamista koskeva säännös koskisi muun muassa viranomaisten välistä viestintää sähköisten tiedonsiirtomenetelmien, kuten sähköpostin, avulla. Tunnistamisella tarkoitetaan esim. vahvaa sähköistä tunnistusmenetelmää.

Ehdotuksen taloudellisia vaikutuksia koskevassa luvussa lähdetään siitä, että ehdotukseen sisältyvät tietoturvallisuutta koskevat säännökset (4 luku) vastaavat pitkälti myös voimassa olevaa lainsäädäntöä sekä pitkälti myös olemassa olevia käytäntöjä. Lisäksi lähdetään siitä, että myöskään muille toimijoille kuin puhtaasti viranomaisille ei ehdotuksella arvioida olevan taloudellisia vaikutuksia, koska niihin sovelletaan julkisuuslakia ja EU:n tietosuoja-asetusta.

Eläketurvakeskuksen näkemyksen mukaan 14 §:n mukainen velvoite siitä, että vastaanottaja tunnistettaisiin vahvalla sähköisellä tunnistusmenetelmällä viranomaisten välisessä sähköpostitietojenvaihdossa, olisi merkittävä muutos nykytilaan. Nykyisin salassa pidettävien henkilötietojen siirto ennalta määriteltyjen yhteistyötahojen kanssa hoidetaan salatulla sähköpostiyhteydellä. Salatulla sähköpostiyhteydellä tapahtuva tietojenvaihto on Eläketurvakeskuksen ja muiden työeläketoimijoiden toiminnassa päivittäistä ja koskee useita viranomaisia, mukaan lukien ulkomaisia viranomaisia, jotka myös ovat pitäneet salattua sähköpostiyhteyttä riittävän tietoturvallisena tapana siirtää toiselle viranomaiselle salassa pidettäviä tietoja.

Henkilöiden välisessä sähköpostissa vaatimus vastaanottajan erillisestä tunnistamisesta tai varmistamisesta, ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja, on haasteellinen. Ominaisuuden vaatiminen rajaa huomattavasti käytettävissä olevia tietojärjestelmiä ja estää esim. yleisesti käytössä olevien sähköpostijärjestelmien käytön. Näin ollen vaatimuksen toteuttaminen edellyttäisi toimijoilta uusia toimintatapoja ja tietojärjestelmien vaihtoa, mistä aiheutuisi kustannuksia. Eläketurvakeskus katsoo, että nykyinen työeläkejärjestelmän käytössä oleva henkilöiden välinen suojattu tiedonsiirto on riittävän tietoturvallista. Ks. tarkemmin liite.

Lakiosasto
Jaana Rissanen

25.1.2019

Eläketurvakeskus katsoo, että 14 §:n mukainen velvoite ei ole nykylainsäädännön mukainen, vaan täysin uusi velvoite. Käsityksemme mukaan myöskään tietosuojavaltuutettu ei ole tällaista edellyttänyt. Ehdotettu vaatimus on lisäksi tiukempi kuin mitä EU:n tietosuoja-asetuksessa edellytetään. Tietosuoja-asetus lähtee rekisterinpitäjän riskiarvioinnista. Tämä tarkoittaa, että rekisterinpitäjän tehtävänä on arvioida millaiset suojatoimet kulloinkin ovat riittäviä. Kansallisessa lainsäädännössä ei pitäisi asettaa tarkempia tietoturvavelvoitteita esimerkiksi viranomaisten tai muiden julkisten toimijoiden väliseen sähköpostiyhteydenpitoon.

Ehdotuksessa tiedonhallintalain ja tietosuoja-asetuksen välistä suhdetta on käsitelty suppeasti. Tietosuoja-asetuksen ja tiedonhallintalain välisen suhteen arvioiminen olisi merkityksellistä tiedonhallintalain koko 4 luvun (tietoturvallisuus) säännösten osalta, koska tietoturvallisuuteen liittyvästä riskien arvioinnista on säädetty tietosuoja-asetuksessa. Tietosuojavaltuutettu on nimenomaisesti todennut lausunnossaan tiedonhallintalain hallituksen esityksen 4 lukuun sisältyvästä 13 §:stä, että säännös näyttäisi osittain päällekkäiseltä sääntelyltä suhteessa tietosuoja-asetuksen 32 artiklaan.

Ehdotuksessa viitataan siihen, että tietosuoja-asetus mahdollistaa sen, että jäsenvaltio voi ottaa käyttöön yksityiskohtaisempia säännöksiä, joilla varmistetaan laillinen ja asianmukainen tietojenkäsittely (tietosuoja-asetuksen 6 artiklan 2 kohta). Jos esityksen tavoitteena on tämän säännöksen perusteella asettaa kansallisessa lainsäädännössä tiukempia vaatimuksia kuin mitä tietosuoja-asetus edellyttää, tulisi tämä käydä selkeästi ilmi hallituksen esityksestä. Esityksessä ei käy riittävällä tavalla ilmi, että miten se täydentää ja täsmentää tietosuoja-asetusta.

Lisäksi Eläketurvakeskus toteaa, että perustuslakivaliokunta on katsonut (PeVL 14/2018 ja 48/2018), että tietosuoja-asetuksen yksityiskohtainen sääntely muodostaa yleensä riittävän säännöspohjan myös perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Näin ollen erityislainsäädäntöön ei ole tietosuoja-asetuksen soveltamisalalla enää valtiosääntöisistä syistä välttämätöntä sisällyttää kattavaa ja yksityiskohtaista sääntelyä henkilötietojen käsittelystä.

Edellä mainitulla perusteilla Eläketurvakeskus katsoo, että 14 §:n mukainen vaatimus pitäisi poistaa hallituksen esityksestä ja muutenkin miettiä koko 4 luvun säännösten tarpeellisuutta ottaen erityisesti huomioon tietosuoja-asetuksen säännökset.

Lakiosasto
Jaana Rissanen

25.1.2019

LIITE

1. Vastaanottajan vahva tunnistaminen

Vastaanottajan vahva tunnistaminen (kaksivaiheinen tunnistaminen vaatii sekä esim. salasanan että matkapuhelimeen tulevan PIN-koodin) on käytettävissä yleisesti. Lakiehdotuksen yksityiskohtaisissa perusteluissa edellytetty ominaisuus, jossa lähettäjä pystyy varmistamaan vastaanottajan ennen kuin vastaanottaja pääsee käsittelemään lähetettyä viestiä, on harvinainen. Eläketurvakeskuksen tietojen mukaan vain Deltagonin Sec@GW- turvaposti toteuttaa vaatimuksen. Sec@GW-turvaposti mahdollistaa ST IV luokitellun tiedon välittämisen. Ominaisuuden vaatiminen rajaa siis huomattavasti käytettävissä olevia tietojärjestelmiä ja estää esim. yleisesti käytettävissä olevien sähköpostijärjestelmien käytön.

2. Henkilöiden välinen tiedonsiirto eläkejärjestelmässä

Henkilöiden välisessä luottamuksellisen tiedon siirrossa työeläketoimijoiden välillä käytetään suojattuja tietoliikenneyhteyksiä tai viesti välitetään salattuna (TLS) siten, että lähettävä järjestelmä salaa viestin ja vastaanottava järjestelmä purkaa viestin automaattisesti vastaanottajan postilaatikkoon.

Viestin vastaanottavan organisaation vastuulla on varmistaa, että ko. postilaatikkoa pääsee lukemaan vain se henkilö, jolle postilaatikko kuuluu.

Työeläketoimijat käyttävät paljon yhteispostilaatikoita, joihin lähetetään tiettyyn asia-alueeseen liittyvät viestit. Käytännössä vaatimus viestin vastaanottajan varmistamisesta estäisi yhteispostilaatikoiden käytön ja siten vaatisi muutoksia nykyisin käytössä oleviin toimintatapoihin.

Käytännössä prosessi menee seuraavasti:

- Lähettäjä lähettää viestin vastaanottavan toimijan osoitteeseen (tyypillisesti etunimi.sukunimi@toimija.fi tai yhteispostilaatikko@toimija1.fi), eikä henkilökohtaisia verkkotunnuksia (”siviilisähköpostin osoite”) käytetä.
- Viesti lähetetään joko suojatulla tietoliikenneyhteydellä tai salattuna
- Vastaanottaja on kirjautunut organisaationsa tietojärjestelmään sisään ja vastaanottava organisaatio vastaa siitä, etteivät muut henkilöt pääse kirjatumaan ”väärinä henkilöinä”.