29.1.2019

Suopelto Kirsi

FINANSSIALA

Eduskunnan hallintovaliokunta (HaV)

HE 284/2018 vp Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Vastaanottajan tunnistamisvaatimus poistettava esityksestä yksityisten toimijoiden osalta

- FA kannattaa esityksen lähtökohtaisia tavoitteita.
- Tiedonhallintalain 4 luvun14 §:n mukainen vaatimus vastaanottajan tunnistamisesta on poistettava esityksestä yksityisten toimijoiden osalta.
- Olisi syytä arvioida yleisemminkin 4 luvun säännösten tarpeellisuutta yksityisten toimijoiden kannalta.

1 Vastaanottajan tunnistamisvaatimus poistettava

Esitetyssä tiedonhallintalain 4 luvun 14 §:ssä säädetään tietojen siirtämisestä tietoverkossa. Säännöksen mukaan viranomaisen on järjestettävä salassa pidettävän tiedon siirto siten, että vastaanottaja varmistetaan tai tunnistetaan tietoverkossa. Pykälän yksityiskohtaisissa perusteluissa puolestaan todetaan, että tunnistamista ja varmistamista koskeva säännös koskisi muun muassa viranomaisten välistä viestintää sähköisten tiedonsiirtomenetelmien, kuten sähköpostin, avulla. Tunnistamisella tarkoitetaan esimerkiksi vahvaa sähköistä tunnistusmenetelmää.

Esityksen taloudellisia vaikutuksia koskevassa luvussa lähdetään siitä, että esityksen 4 luvun tietoturvallisuutta koskevat säännökset vastaavat pitkälti voimassa olevaa lainsäädäntöä sekä olemassa olevia käytäntöjä. Myöskään muille toimijoille kuin puhtaasti viranomaisille ei ehdotuksella arvioida olevan taloudellisia vaikutuksia, koska niihin sovelletaan julkisuuslakia ja EU:n tietosuoja-asetusta. Tämä ei pidä paikkaansa. Tämä olisi tullut valmistelussa esille, jos lakisääteistä vakuutustoimintaa harjoittavia toimijoita olisi valmistelun aikana kuultu.

Sääntely koskee myös lakisääteisiä vakuutuksia tarjoavia yksityisiä vakuutusyhtiöitä ja työeläkelaitoksia niiden käyttäessä julkista valtaa vakuutustoiminnassaan. Vakuutusyhtiöiden välistä tiedonvaihtoa 4 luvun 14 §:n tarkoittamalla tavalla tapahtuu sähköpostin välityksellä säännöllisesti päivittäin. Kyseessä ovat yleensä yksittäiset kyselyt eri vakuutusyhtiöitä edustavien luonnollisten henkilöiden (toimihenkilö/virkailija) välillä.

Esimerkiksi työtapaturmavakuutuksen korvauskäsittelyssä tietojen vaihtoa tapahtuu useimmiten liikennevakuutusta toimeenpanevien laitosten, Kelan, työeläkelaitosten, Eläketurvakeskuksen tai työttömyyskassojen välillä. Tietojen vaihdossa on yleensä kyse siitä, että vaikkapa työeläkelaitos tai Kela tiedustelee työtapaturmavakuutuslaitokselta, tuleeko se myöntämään työtapaturma- ja ammattitautilain mukaista etuutta vastaavalle ajalle kuin se olisi itse myöntämässä. Tietojenvaihto ja tietojen siirtäminen liittyy siten eri sosiaaliturvaetuuksien yhteensovittamiseen tai etuuksien huomioon ottamiseen. Tietojen vaihto liittyy eri sosiaaliturvajärjestelmistä käsiteltävänä olevan etuudensaajan asian käsittelyyn ja tietojenvaihto on etuudensaajan edun mukaista.

Tietojenvaihto sähköpostitse tehdään aina salattua tai muuten suojattua yhteyttä käyttäen. Tiedon vastaanottajana voi olla toimijaa edustava yksittäinen toimihenkilö (etunimi.sukunimi@viranomainen.fi) tai vastaanottajana voi toimia asiaa hoitava ryhmä, jolloin käytössä on ns. yhteis-/ryhmäsähköpostilaatikko (yhteissähköpostilaatikko@viranomainen.fi). Yhteissähköpostilaatikoita käytetään, koska lähettävän organisaation ei voida edellyttää tietävän miten työnjako vastaanottavassa organisaatiossa kulloinkin on järjestetty ja jotta varmistetaan vastaanotettujen tietojen käsittely myös toimihenkilön poissaolo- ja loma-aikoina. Yhteissähköpostilaatikoiden lukuoikeuksia rajataan tehtävän mukaisilla käyttöoikeuksilla.

Vaatimuksen toteuttaminen edellyttäisi toimijoilta uusia toimintatapoja ja tietojärjestelmien vaihtoa, koska nykyisillä yleisesti käytössä olevilla sähköpostivälineillä ei vaatimusta voida toteuttaa. Tästä aiheutuisi toimijoille merkittäviä kustannuksia ja edellyttäisi tarkkaa vaikutusten arviointia. Käytännössä vaatimus viestin vastaanottajan varmistamisesta voisi estää yhteissähköpostilaatikoiden käytön ja siten vaatisi muutoksia nykyisin käytössä oleviin tehokkaisiin toimintatapoihin. Vaatimus voisi myös johtaa siihen, että sähköpostin käytöstä jouduttaisiin luopumaan ja tiedonsiirto jouduttaisiin tekemään perinteisesti kirjepostilla tai puhelimitse. Näidenkin osalta jää epäselväksi, miten tiedon vastaanottaja tunnistettaisiin riittävän tietoturvallisesti. Pahimmillaan tällaiset toimintatavat myös hidastaisivat etuuskäsittelyä.

Esitetyn 4 luvun 14 § vaatimus siitä, että vastaanottaja tulisi varmistaa ja tunnistaa riittävän tietoturvallisella tavalla on edellä kerrotulla tavalla uusi vaatimus nykytilaan nähden. Lakisääteisiä vakuutuksia tarjoavien yksityisten vakuutusyhtiöiden tietojenvaihtoa säännellään tietosuoja-asetuksen ja kansallisen tietosuojalain lisäksi esimerkiksi sektorikohtaisessa erityissääntelyssä sekä Finanssivalvonnan antamin määräyksin. Missään niissä ei aseteta toimijoille näin tarkkarajaista vaatimusta.

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, eikä kansallisessa lainsäädännössä pitäisi asettaa tarkempia tietoturvavelvoitteita esimerkiksi viranomaisten tai muiden julkisten toimijoiden väliseen sähköpostiyhteydenpitoon. Käsityksemme mukaan myöskään tietosuojavaltuutettu ei ole tällaista edellyttänyt, vaan päinvastoin katsoo, että päällekkäinen kansallinen sääntely ei ole tietosuoja-asetuksen mukaista. Näin ollen **FA:n näkemyksen mukaan esityksestä tulisi poistaa vastaanottajan tunnistamista koskeva vaatimus lakisääteisiä vakuutuksia tarjoavien yksityisten toimijoiden osalta.**

2 Esityksen 4 luvun suhde tietosuoja-asetukseen

Esityksestä ei käy riittävällä tavalla ilmi ehdotettavan tiedonhallintalain ja tietosuoja-asetuksen välisen sääntelyn suhde ja miltä osin tiedonhallintalaki täydentää ja täsmentää tietosuoja-asetusta. Esitettyyn tiedonhallintalain 4 lukuun sisältyvät vaatimukset ovat tiukempia kuin mitä tietosuoja-asetuksessa edellytetään. Mikäli kansallisessa lainsäädännössä on tarkoitus asettaa tiukempia ja tarkkarajaisempia vaatimuksia kuin mitä yleinen tietosuoja-asetus edellyttää tämän tulisi käydä selkeämmin ilmi hallituksen esityksestä.

Myös perustuslakivaliokunta on katsonut (PeVL 14/2018 ja 48/2018), että tietosuoja-asetuksen yksityiskohtainen sääntely muodostaa yleensä riittävän säännöspohjan 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.

Kun lakisääteisen vakuuttamisen toimeenpanossa käytetään julkista valtaa, tiedot ja asiakirjat ovat pääsääntöisesti salassa pidettäviä. Tietoja luovutetaan vain kyseistä vakuutuslajia koskevien erityislakien säännösten tai muussa laissa olevan säännöksen perusteella. Lisäksi Finanssivalvonta ohjaa antamillaan määräyksillä alan toimijoita myös tietoturvan osalta ja valvoo niiden toimintaa. Lakisääteisten vakuuttajien toiminnassa tietoturvallisuus on vakiintuneesti otettu huomioon ja tietoturvallisuutta koskevat velvoitteet tulevat suoraan tietosuoja-asetuksesta ja tietosuojalaista. Lakiesityksen mukainen yksityiskohtainen lisäsääntely ei siten ole tarpeen lakisääteisten vakuuttajien osalta.

FA:n näkemyksen mukaan tulisikin harkita, onko esitetty 4 luku tarpeen ottaen huomioon tietosuoja-asetus ja kansallinen tietosuojalaki sekä lakisääteistä vakuuttamista ohjaava erityissääntely ja viranomaismääräykset. Lisäsääntely saattaa luoda riskin epäselvästä oikeustilasta ja johtaa käytännössä hankaliin tulkintatilanteisiin.

FA on laatinut lausunnon yhteistyössä Tapaturmavakuutuskeskuksen, Liikennevakuutuskeskuksen sekä Työeläkevakuuttajat ry:n kanssa, joiden yhteinen kanta on kirjattu lausuntoon.

FINANSSIALA RY

Lea Mäntyniemi