Finanssiala ry

Lausunto

03.03.2021

Asia: VN/3501/2021

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; lausuntopyyntö (Huom! Lausuntoaika päättyy 3.3.2021)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

LIIKENNE- JA VIESTINTÄMINISTERIÖLLE

FINANSSIALA RY:N LAUSUNTO LUONNOKSESTA VALTIONEUVOSTON PERIAATEPÄÄTÖKSEKSI TIETOTURVAN JA TIETOSUOJAN PARANTAMISEKSI YHTEISKUNNAN KRIITTISILLÄ TOIMIALOILLA (DIAARINUMERO: VN/24348/2020)

Liikenne- ja viestintäministeriö on 2.3.2021 pyytänyt Finanssiala ry:n lausuntoa luonnoksesta valtioneuvoston periaatepäätökseksi tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (jäljempänä periaatepäätösluonnos).

1. Finanssiala ry (FA) pitää tärkeänä, että tietoturvaa ja tietosuojaa pyritään suunnitelmallisesti ja johdonmukaisesti parantamaan sekä yksityisellä että julkisella sektorilla.

2. Periaatepäätösluonnoksessa esitetyt sääntelytarpeet, toimenpiteet ja niiden hallinnolliset kustannukset näyttävät voimakkaasti kohdentuvan yksityiselle sektorille. FA pitää erittäin valitettavana, ettei yksityistä sektoria kuitenkaan ole otettu mukaan periaatepäätöstä valmistelleeseen työryhmään eikä elinkeinoelämän kommentteja työryhmän väliraporttiin juurikaan näytä huomioidun periaatepäätösluonnoksessa. FA pitää myös periaatepäätösluonnoksen kommentoinnille varattua puolentoista päivän lausuntoaikaa kohtuuttoman lyhyenä ja hyvän säädösvalmistelun perusperiaatteiden vastaisena.

3. Kuten periaatepäätösluonnoksessakin todetaan, finanssisektori on varautunut hyvin tietoturva- ja tietosuojauhkiin. Huoltovarmuuskeskuksen syksyllä 2020 julkaistun selvityksen ”Kyberturvallisuuden nykytila eri toimialoilla” perusteella kyberturvallisuuden tila finanssisektorilla (4.20/5.00) oli selvästi paras ja esimerkiksi teleliikennealaa (3.96), ICT- ja ohjelmistoalaa (3.86),

energia-alaa (3.73) ja terveydenhoitoalaa (3.69) selvästi parempi. Tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla selvittäneen työryhmän loppuraportissa todetaan, että viranomaisvalvonnassa saatujen havaintojen perusteella myös tietosuojan osalta vahvasti säännellyt alat (kuten finanssisektori) ovat valveutuneimpia ja paremmin resursoituja, mikä näkyy mm. tietoturvailmoituksissa ja tietoisuudessa sääntelyn vaatimuksista ja niiden noudattamisesta. FA:n näkemyksen mukaan mahdollisten uusien toimenpiteiden painopisteen tuleekin olla niillä sektoreilla ja julkisen sektorin yksiköissä, joissa on havaittu puutteita ja kehittämistarpeet ovat suurimmat.

4. Termi ”yhteiskunnan kriittiset toimialat” on luonteeltaan kuvaileva eikä sitä ole määritelty lainsäädännössä. Jos termiä halutaan käyttää sääntelytarkoituksissa, sen sisältöä ei FA:n näkemyksen mukaan tule jättää asiayhteydestä pääteltäväksi, vaan termi tulee määritellä yksiselitteisesti. Sekaannusten välttämiseksi määritelmän tulisi myös olla yhteensopiva huoltovarmuuden turvaamista ja kansallista turvallisuutta koskevien sääntelyjen kanssa. FA pitää tärkeänä, että terminologia on yksiselitteistä ja linjauksista käy selvästi ilmi, miltä osin kyse on elinkeinoelämään ja miltä osin viranomaisiin kohdistuvista vaatimuksista.

5. Finanssitoimialan osalta FA pitää tärkeänä, että periaatepäätöksessä huomioidaan toimialaan jo kohdistuvan EU-sääntelyn ohella myös vireillä olevat lainsäädäntöhankkeet, kuten verkko- ja tietoturvadirektiivin päivittäminen ja rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskevan asetuksen antaminen. Periaatepäätöksessä esitettävät toimenpiteet eivät myöskään saa olla ristiriidassa esimerkiksi Euroopan keskuspankin, Euroopan finanssivalvojien, Kansainvälisen arvopaperimarkkinavalvojien yhteisön tai Finanssivalvonnan toimivaltuuksien tai niiden antaman sääntelyn kanssa. Huomiota tulee lisäksi kiinnittää FA:n henkilötietojen käsittelyä finanssialalla koskeviin käytännesääntöihin, jotka määrittävät henkilötietojen käsittelyn periaatteet, edistävät hyvää henkilötietojen käsittelytapaa ja pyrkivät lisäämään asiakkaiden luottamusta finanssitoimialaan.

6. Kokemukset finanssialalta osoittavat, että tietoturva- ja tietosuojaloukkausten ehkäisemisen, havaitsemisen ja selvittämisen kannalta alan toimijoiden ja palveluntuottajien välinen tietojenvaihto on vähintään yhtä tärkeää kuin viranomaisten välinen tietojenvaihto. Tämän vuoksi on ensiarvoisen tärkeää, että viranomaisten välistä yhteistyötä koskevaa sääntelyä tarkennettaessa myös elinkeinoelämän toimijoiden strategista, taktista ja operatiivista tietojenvaihtoa koskevat säännöt selkeytetään ja tietoturva- ja tietosuojauhkien torjunnan edellyttämälle tietojenvaihdolle luodaan tukeva säädöspohja.

7. Periaatepäätösluonnoksen linjauksessa 4 esitetään, että Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen (KTK) resursseja vahvistetaan, jotta se pystyy antamaan riittävästi apua ja toimialakohtaista neuvontaa muille hallinnonaloille. FA pitää ehdotusta sinänsä hyvänä, mutta vastuuvirkamiesten toimialakohtaista neuvontaa ei pidä rajata vain sektoriviranomaisille, vaan se tulee ulottua myös asianomaisen toimialan yrityksiin. On myös välttämätöntä, että KTK:n resurssien riittävyys varmistetaan niin, etteivät mahdolliset uudet tehtävät vaaranna nykyistä hyvin sujuvaa yhteistyötä mm. finanssialan toimijoiden kanssa.

8. Periaatepäätösluonnoksen linjauksessa 5 mainittujen KTK:n koulutustehtävien osalta on huomattava, että tietoturvallisuuden ja tietosuojan toimintaympäristöt ja uhkakuvat muuttuvat jatkuvasti, joten koulutuksen tarve on jatkuva, mikä tulee edellyttämään merkittäviä panostuksia KTK:n resursseihin. Koulutuksen tarve ei myöskään rajoitu vain tietoturvavalvonnan parissa työskenteleviin, vaan sen tulee riittävässä laajuudessa kattaa koko henkilöstö. Vaihtoehtona voisi

olla virastokohtaisten tietoturvapäälliköiden nimeäminen, joiden vastuulla olisi huolehtia virastonsa henkilöstön tietoturvakoulutuksesta.

9. Periaatepäätösluonnoksen linjauksessa 6 esitetty tietoturvallisuuden kartoituspalvelun laajentaminen edellyttänee panostuksia myös kartoituspalvelun käyttäjien tukeen. Pelkkä tieto mahdollisesta ulkoverkon haavoittuvuudesta ei riitä, vaan erityisesti pienemmissä organisaatioissa tarvitaan ohjausta myös siitä, mihin toimenpiteisiin tulisi ryhtyä tilanteen korjaamiseksi.

10. Tarve periaatepäätösluonnoksen linjauksessa 7 ehdotetuille yhdenmukaisille, kattaville, luotettaville ja turvallisille käsittely-ympäristöille ja tiedonsiirtopalveluille on ilmeinen ja ne tulisi toteuttaa mahdollisimman nopealla aikataululla. Hallinnonalojen sisäisten ja välisten siirtojen ohella ratkaisujen tulisi mahdollistaa myös mm. hallinnonalojen ja yritysten väliset tietojen siirrot.

11. FA kannattaa periaatepäätösluonnoksen linjauksessa 8 esitettyä Havaro-palvelun käyttäjäpiirin laajennusta.

12. Periaatepäätösluonnoksen linjauksen 9 osalta FA pitää selvänä, että elinkeinoelämän toimijoita velvoittavien tietoturvavaatimusten tulee olla selkeitä, oikeasuhtaisia, lakiin perustuvia sekä Suomea koskevien EU- ja kansainvälisoikeudellisten velvoitteiden mukaisia. Linjauksessa esitetty tietoturvaa koskevien sitovien määräysten antovaltuuksien delegointi asetustakin alemmalle tasolle on ylimitoitettua ja hyvän sääntelyn periaatteiden vastaista. Muutokset tietoturvan ja tietosuojan kannalta merkityksellisissä teknisissä tai toiminnallisissa järjestelyissä edellyttävät usein merkittäviä taloudellisia panostuksia, minkä vuoksi tällaisista velvoitteista tulee ehdottomasti säätää lain tasolla.

13. Periaatepäätösluonnoksen linjauksissa 12, 13 ja 14 esitetään tarkemmin määrittelemättömälle joukolle kriittisten toimialojen suurimpia ja merkittävimpiä toimijoita erittäin pitkälle meneviä kansallisia velvoitteita määritellä, dokumentoida, luokitella, auditoida ja sertifioida tieto- ja tietoliikenneteknisiä prosessejaan ja toimintojaan. Vaatimukset näyttäisivät merkittävällä tavalla puuttuvan ainakin elinkeinonvapauteen, mitä tuskin voidaan pitää perusteltuna, tarpeellisena tai edes mahdollisena. Toteutuessaan tämänkaltaiset liiketoiminnan tarpeet ylittävät velvoitteet voivat johtaa siihen, että palvelujen tarjonta siirtyy kansallisen lisäsääntelyn ulottumattomiin Suomen rajojen ulkopuolelle. Jos linjauksissa ehdotettuja vaatimuksia halutaan edistää, niistä saatavat hyödyt on kyettävä osoittamaan. Lisäksi on varmistettava, että velvoitteet ovat oikeasuhtaisia eikä niistä aiheudu toimijoille kohtuutonta taloudellista, hallinnollista tai toiminnallista rasitusta.

14. Periaatepäätösluonnoksen linjauksen 19 osalta FA pitää välttämättömänä, että periaatepäätöksessä ja sen pohjalta mahdollisesti valmisteltavassa lainsäädännössä varmistetaan, että Liikenne- ja viestintävirastolla on eri liikennemuotojen tietoturvaa koskevia määräyksiä antaessaan velvoite tehdä yhteistyötä asianomaisiin liikennemuotoihin liittyviä vakuutuksia myöntävien vakuutuslaitosten kanssa.

15. Periaatepäätösluonnoksen linjausten 20, 21 ja 22 osalta FA pitää tärkeänä, että poliisi- ja valvontaviranomaisille varmistetaan uusien ja laajenevien tehtäviensä edellyttämät resurssit. Mahdollisten lainsäädäntömuutosten yhteydessä tulisi myös kriittisesti arvioida identiteettivarkauden ja muiden tietoverkkorikosten rangaistusasteikkojen riittävyyttä sekä mahdollistaa näihin liittyvien rikosepäilyjen edellyttämät tutkintakeinot ja esimerkiksi esitutkinnan rajaaminen nykyistä laajemmin. Epäiltyjen tietoturva- ja tietosuojaloukkausten raportointikynnyksen alentamiseksi on ensiarvoisen tärkeää laajentaa ja nopeuttaa loukkausten selvittelyä ja esitutkintaa

sekä mitoittaa niihin liittyvät rangaistusasteikot sellaisiksi, että tekijä joutuu aidosti punnitsemaan tekonsa seuraamuksia ennen sen toteuttamista. Nykytilanteessa merkittävä osa ilmoitetuistakin tietoverkkorikoksista jäänee tutkimatta, jolloin uhrin kannalta rikosepäilyn ilmoittaminen merkitsee vain tarpeetonta lisätyötä.

16. Periaatepäätösluonnoksen linjausten 24, 25, 26, 27, 28 ja 29 osalta FA pitää tärkeänä, että tietoturvallisuus- ja tietosuojavaatimukset otetaan vakavasti myös julkisella sektorilla. Julkisuudessa kuvattujen kaltaiset potilastietojen vuodot, poliisin tietojärjestelmien luvattomat hyödyntämiset yksityisiin tarkoituksiin, Lahden, Porin ja Kokemäen tietojärjestelmien lamaantumiset, kyvyttömyys suojautua viranomaisten palveluja lamauttaneilta palvelunestohyökkäyksiltä, ulkoministeriöön kohdistunut tietomurto, jne. osoittavat, etteivät haasteet rajoitu vain yksityisen sektorin toimijoihin.

FA haluaa erityisesti kiinnittää huomiota siihen, että tietotuvallisuuden ja tietosuojan parantamisessa on keskeisesti kyse organisaation toimintakulttuurin ja -tapojen kehittämisestä sekä oletusarvoisten ja sisäänrakennettujen tietosuoja- ja tietoturvallisuusvaatimusten huomioimisesta uusia järjestelmiä ja prosesseja kehitettäessä ja käyttöönotettaessa. Ehdotus näiden vaatimusten huomioimisesta jo hankintojen yhteydessä on sen vuoksi erittäin kannatettava, koska jälkeenpäin niiden toteuttaminen voi olla vaikeaa tai jopa mahdotonta.

Tietoturvallisuuden osalta on selvää, ettei kyse ole Valtorille tai muulle palveluntuottajalle ulkoistettavissa olevasta teknisestä ongelmasta, vaan finanssisektorin tapaan viimesijaisen vastuun tulee aina olla palveluja ulkoistavalla valtionhallinnon toimijalla.

17. Periaatepäätösluonnoksen linjausten 30 ja 31 osalta FA haluaa kiinnittää huomiota siihen, että Suomessa on valittu linja, jonka mukaan tietosuoja-asetuksen sanktioita ei kohdisteta julkiseen sektoriin. Tämä näyttäisi johtaneen siihen, ettei tietosuojan tasoon ole ollut tarpeen kiinnittää niin suurta huomioita julkisella sektorilla eikä siihen myöskään ole varattu tarpeeksi resursseja. Jos sanktiot koskisivat yhtäläisesti kaikkia toimijoita, tilanne olisi parempi tietosuojan tason suhteen. FA:n mielestä tietosuoja-asetuksen sanktioiden ulottamista julkiseen sektoriin tulisikin arvioida tässä yhteydessä uudelleen. FA pitää myös tarpeellisena, että linjauksissa ehdotetut kyvykkyystasojen arvioinnit ja tietosuojaa koskevat vaikutusarvioinnit ulotetaan myös julkisen sektorin toimijoihin.

18. Periaatepäätösluonnoksen linjauksen 32 osalta FA pitää tarpeellisena, että Suomessakin saataisiin pikaisesti käyttöön ulkopuolisten tahojen myöntämät sertifioinnit, joilla rekisterinpitäjät voisivat osoittaa vaatimusten noudattamisen. Vaikka sertifioinnit ovat kalliita, niiden tuomat hyödyt ja kustannukset tulisi suhteuttaa tietosuojaa koskevien vaatimusten noudattamisesta koituviin ja usein huomattaviksi nouseviin kokonaiskustannuksiin.

19. Periaatepäätösluonnoksen linjaukseen 33 sisältyvien standardointi- ja niihin liittyvien auditointivelvoitteiden osalta FA pitää tärkeänä, että lainsäädännössä yksilöidään, mikä taho ja mitä menettelyä noudattaen määrittelee kyseeseen tulevat standardit. Standardit on määriteltävä yksiselitteisesti, jotta toimijoilla on mahdollisuus huomioida vaatimukset omissa toimintaprosesseissaan ja ICT-sopimuksissaan. FA:n näkemyksen mukaan standardit eivät myöskään voi olla puhtaasti kansallisia (esim. Suomen kansalliset KATAKRI-, PITUKRI- tai VAHTI-ohjeet ja standardit), vaan samojen sääntöjen tulee soveltua läpi palvelu- ja hankintaketjujen siitä riippumatta, missä päin yhteismarkkinoita toimintaa harjoitetaan, asiakkaat sijaitsevat, palveluja tarjotaan tai alihankkijat toimivat.

20. Periaatepäätösluonnoksen linjauksen 35 mukaisesti FA pitää tärkeänä, että Tietosuojavaltuutetun toimiston resurssit turvataan määrällisesti ja laadullisesti ja mahdollisia uusia

tehtäviä asetettaessa varmistetaan, etteivät ne vaaranna nykyisten tehtävien asianmukaista hoitamista.

21. Periaatepäätösluonnoksen linjauksen 37 osalta FA pitää järkevänä ja tarpeellisena, että periaatepäätösluonnoksessa ehdotettua mobiilipäätelaitteeseen asennettavaa sovellusta kehitettäessä lähtökohdaksi otettaisiin se, että ilmoitus tietoturvaloukkauksesta voidaan samalla kertaa tehdä kaikille asiaan liittyville viranomaisille. Tarvittaessa viranomaisten menettelytavat ja raportointialustat tulisi yhdenmukaistaa niin, että yksi ilmoitus riittäisi ja toimija voisi keskittyä ongelman pikaiseen ratkaisemiseen sen sijaan, että rajallisia resursseja käytetään ilmoitusten laatimiseen. Samalla olisi luontevaa sallia ilmoituksen tekeminen myös englanniksi, mikä helpottaisi ja nopeuttaisi erityisesti monikansallisten toimijoiden raportointia.

22. Edellä todetun mukaisesti FA haluaa lopuksi kiinnittää huomiota siihen, että periaatepäätösluonnoksessa kuvatut säädös- ja toimenpide-ehdotukset edellyttäisivät huomattavia panostuksia sekä elinkeinoelämän että viranomaisten puolella. Tämän vuoksi FA pitää välttämättömänä, että niiden taloudelliset ja hallinnolliset kustannukset ja toteuttamiskelpoisuus arvioidaan mahdollisimman luotettavasti sekä periaatepäätöksen jatkokäsittelyn että mahdollisten lainsäädäntöhankkeiden yhteydessä.

FINANSSIALA RY

Taina Ahvenjärvi

Linna Mika
Finanssiala ry