Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Lausunto

06.09.2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Liikenne- ja viestintävirasto Traficom katsoo, että arviomuistiossa esitetty nykytilakuvaus on päälinjojen osalta osuva. Muutamien kirjausten osalta vaikuttaisi kuitenkin esiintyvän yksittäisiä epätarkkuuksia ja tulkinnanvaraisuuksia, jotka on huomioitu lausunnon kyseisessä asiayhteydessä. Traficom kiinnittää huomiota siihen, että nykyinen arviointitoimintaa koskeva sääntely ja sen mukaiset toimintamallit eivät ole kaikille käyttäjäorganisaatioille tuttuja, mikä on omiaan aiheuttamaan väärinkäsityksiä ja sekaannusta.

Traficom nostaa esille, että arviomuistion ja siihen saatujen lausuntojen pohjalta tehtävässä jatkotyössä tulisi selkeästi huomioida myös kesäkuussa 2021 hyväksytty valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Liikenne- ja viestintävirasto Traficom pitää tärkeänä, että tietojärjestelmiä koskevassa sääntelyssä otetaan huomioon vaatimukset, joilla varmistetaan, että uudet tietojärjestelmät täyttävät teknisten vaatimusten lisäksi myös hallintolain ja hyvän hallinnon vaatimukset. Erityisesti tietojärjestelmien kehitystyössä tulisikin huomioida, että vaikka kehitystyö voidaan tehdä tekninen toteutus edellä, hyvän hallinnon periaatteet sekä esimerkiksi hallintolain, julkisuuslain ja kielilain vaatimukset tulevat huomioiduiksi.

Traficom nostaa esille, että hallintoasian vireille panijalle voi olla erityistä merkitystä sillä, että hän saa tiedon siitä, onko päätös tehty automaattisesti. Koska automaattiseen päätöksentekoon voi sisältyä virhetilanteita, voi hakija arvioida muutoksenhaun tarvetta ja perusteita tämän tiedon perusteella. Jatkotyössä olisi hyvä arvioida myös sitä, muodostaako automaattisen käsittelyn perusteella annettu päätös missään tilanteessa suoraan oikeutta hakea muutosta hallinto-oikeudesta ilman, että siitä olisi oikeus saada hakea oikaisua päätöksen tehneeltä viranomaiselta.

Traficom pyytää kiinnittämään huomiota myös arviomuistiossa esitettyyn näkemykseen siitä, että automaattisen päätöksenteon algoritmeja ei olisi tarpeen ilmaista asianosaiselle. Hallintopäätös tulee perustella riittävän huolellisesti hallintolain mukaan. Koska automaattinen päätöksenteko voi olla sekä viranomaisille, että viranomaispalveluja käyttäville entuudestaan heikosti tunnettu asia,

olisi jatkotyössä hyvä täsmentää automaattisen päätöksenteon perustelujen antamisvelvoitetta ja niiden suhdetta päätöksentekosäännöstöön, mukaan lukien algoritmeihin. On myös huomioitava, että päätöksen perusteluvelvollisuus ei aina toteudu sillä, että asianosaiselle ilmoitetaan asiassa sovelletut lainkohdat, vaan voi olla tarve perustella sitä, miten lainkohtia on tosiasiassa sovellettu asianomaisen tapauksessa.

Traficom pitää tärkeänä, että automaattisen päätöksenteon ja virkavastuun suhdetta täsmennetään. Vaikka tiedonhallintayksikön johto on tiedonhallintalain (906/2019, 4 §) mukaisesti kokonaisvastuussa tiedonhallintayksikön toiminnasta, olisi hyvä lisäksi määritellä millaisissa tilanteissa yksittäinen virkamies on vastuussa automaattisen päätöksenteon toimenpiteistä. Määrittelyssä olisi hyvä huomioida erityisesti tilanteet, joissa yksittäisillä virkamiehillä voi olla vaikutusmahdollisuuksia vain automaattisen päätöksenteon osakokonaisuuksiin.

Traficom nostaa myös esille, että toiminnan riittävän jatkuvuuden varmistamiseksi olisi perusteltua säätää velvollisuus huolehtia asioiden käsittelystä myös tilanteissa, joissa automaattinen päätöksentekoprosessi ei eri tilanteista johtuen toteudu.

Traficom ehdottaa, että sääntelyvalmistelussa huomioitaisiin myös se, miten uudet teknologiat arvioitaisiin päätöksentekoprosessiin liittyvien juridisten vaatimusten osalta ennen niiden käyttöönottoa, mahdollisesti samansuuntaisilla menettelyillä kuin mitä jo sovelletaan sähköisten palveluihin tietoturvallisuuden ja tietosuojaan arviointiin. Traficom näkee tällaisen arvioinnin perustelluksi erityisesti viranomaisella asioivien perusoikeuksien turvaamiseksi.

Traficom nostaa esille myös lokitietojen keräämisen roolin osana tietojen käsittelyprosessin toteutumista ja virkavastuuta. Keskeisten lokitietojen määrittämisen ja keräämisen lisäksi olisi hyvä pohtia myös sitä, millä periaatteilla kerättyjä lokitietoja voidaan jälkikäteen hyödyntää käsittelyprosessin toimivuuden ja oikeellisuuden varmistamiseen. Avoimena kysymyksenä voi esiintyä esimerkiksi se, millä edellytyksillä asianomistajalle voi muodostua oikeus lokitietoihin tutustumiseen.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

-

4. Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

-

5. Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

Liikenne ja viestintävirasto Traficom nostaa esille, että mahdollisten dokumentointivaatimusten olisi hyvä olla mitoitettu kyseisen dokumentaation käyttötarkoitukseen. Dokumentointia ei tulisi edellyttää vain dokumentoinnin vuoksi, vaan dokumentaation tulisi tukea jotain tunnistettua käyttötarkoitusta. Erilaisia käyttötarkoituksia tukevan dokumentaation laadintaan olisi hyvä olla saatavilla myös konkreettisia esimerkkejä, joita voitaisiin julkaista esimerkiksi tiedonhallintalautakunnan suositusten muodossa.

6. Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

-

7. Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

Liikenne- ja viestintävirasto Traficom näkee erittäin kannatettava viranomaistoimintaa tukevan tavoitteen eri tietolähteiden yhdistelemisen mahdollisuuksista, mihin myös jo tiedonhallintalain (906/2019) 20 § ja 22 § osaltaan perustellusti ohjaavat. Samalla tulee kuitenkin huolehtia tietojen laadusta sekä tietojen suojaamisesta koko niiden elinkaaren ajan. Traficom näkisi hyvänä, jos päivittyvässä lainsäädännössä otettaisiin selvästi kantaa myös vastuukysymyksiin tilanteissa, joissa viranomaisen päätöksenteossa on hyödynnetty toiselta viranomaiselta saatuja tietoja, jotka osoittautuvat myöhemmin puutteellisiksi tai jopa virheellisiksi. Jatkotyössä olisi hyvä huomioida myös suhde kansainväliseen yhteistyöhön (vrt. esimerkiksi Euroopan parlamentin ja neuvoston asetus (EU) 2018/1724).

8. Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

Tietojärjestelmien arviointien laajentaminen muihin olennaisiin vaatimuksiin

Traficom näkee perustelluksi arviomuistion ehdotuksen siitä, että tietojärjestelmien arviointia laajennetaan tietoturvallisuuden lisäksi myös muihin tietojärjestelmien ominaisuuksia mittaaviin ominaisuuksiin, toisin sanoen tietojärjestelmien muiden olennaisten vaatimusten täyttymisen arviointeihin. Traficom kuitenkin huomauttaa, että tietoturvallisuuteen ja edellä mainittuihin muihin olennaisiin vaatimuksiin liittyvät viitekehykset, soveltuvat todennusmenetelmät ja esimerkiksi kohdejärjestelmään liittyvien tietojen tietojenkäsittelyn turvallisuuteen kohdistuvat tarpeet eroavat toisistaan merkittävästi.

Traficomin arviointitoimintaa on kehitetty yli kymmenen vuoden ajan, ja sen ydinosaaminen on keskitetty tietojärjestelmien tietoturvallisuuden syvälliseen arviointiin. Traficom näkee, että arviointitoiminnan laajentamisessa tietojärjestelmien arviointiin yleisemmin on kaksi keskeistä etenemisvaihtoehtoa. Ensimmäinen vaihtoehto olisi jatkossakin keskittää Traficomin arviointitoiminta tietojärjestelmien tietoturvallisuuden syvälliseen arviointiin, ja ohjata tietojärjestelmien muiden olennaisten vaatimusten arviointi kaupallisesti toimiville tahoille, mahdollisesti rajautuen arviointilaitoksiin. Mikäli ratkaisumallissa päädyttäisiin hyödyntämään arviointilaitoksia, tämä edellyttäisi maltillisia lisäresursointitarpeita kyseisen pätevyysalueen mukaiseen hyväksyntä- ja valvontatoimeen.

Toinen vaihtoehto olisi laajentaa Traficomin arviointitoiminta kattamaan tietoturvallisuuden lisäksi myös muiden olennaisten vaatimusten arvioinnin. Tämä malli edellyttäisi huomattavia lisäresursointitarpeita Traficomin arviointitoimintaan riippumatta siitä, toteuttaisiko Traficom arviointitoimeksiannot kokonaisuudessaan virkamiestyönä tai käyttäen yksityisiä arvioitsijoita apunaan. Lisäksi tulee huomioida, että Traficom joutuu jo nykyisellään priorisoimaan rajatut resurssinsa yhteiskunnan kannalta kriittisimpiin kohteisiin, mikä myös puoltaisi kaupallisten toimijoiden hyödyntämistä muiden olennaisten vaatimusten ei-turvallisuuskriittisiin arviointeihin.

Tietoturvallisuuden ja muiden olennaisten vaatimusten arvionteihin liittyvien tarpeiden ollessa merkittävän eroavia, Traficom näkee loogisimpana, käytännönläheisimpänä ja myös

kustannustehokkaimpana ratkaisumallina säilyttää tietoturvallisuuden arviointitoiminnan päälinjat ennallaan, ja säätää muiden olennaisten vaatimusten arvioinnista erikseen. Traficom kannattaakin vahvasti ensimmäistä ratkaisumallia, jossa muiden oleellisten vaatimusten arviointi ohjattaisiin kaupallisille toimijoille, mahdollisesti arviointilaitoksille.

Automaattiseen päätöksentekoon liittyvät arvioinnit

Traficom yhtyy arviomuistiossa esitettyyn näkemykseen siitä, että on ongelmallista, mikäli automaattiseen päätöksentekoon käytetyn tietojärjestelmän toiminnallisuuksien ja päätöksentekologiikan oikeellisuuden arviointi siirrettäisiin kyseisen tietojärjestelmän vastuuviranomaisen ulkopuolelle. Kuten arviomuistiossa osuvasti kuvataan, kyseisellä viranomaisella on vastuu lain noudattamisesta ja siten siitä, että järjestelmän toimintalogiikka on lain mukainen. Viranomaisella on myös todennäköisesti paras asiantuntemus toimintalogiikan perusteena olevasta lainsäädännöstä sekä päätöksentekosääntöjen muodostamisesta lain perusteella. Päätöksentekosäännöistä johtuvia virheitä ei välttämättä ulkopuolinen arvioija pysty havaitsemaan – eikä viranomainen voi ulkoistaa sen virkavastuulle kuuluvien päätöksentekosääntöjen laatimista. Traficom ei näekään perustelluksi säätää tällaiselle arvioinnille ulkoista vastuuviranomaista. Traficom ehdottaa sen sijaan, että kyseisestä järjestelmästä vastuussa oleva viranomainen hyödyntäisi ulkoisia, kaupallisia toimijoita arvioimaan järjestelmän teknistä turvallisuutta sekä viranomaisen määrittelemän toimintalogiikan ja sen teknisen toteutuksen vastaavuutta.

Turvallisuusjohtamiseen liittyvien arviointivastuiden selkeyttäminen

Liikenne- ja viestintävirasto Traficom näkee perustelluksi muutosehdotuksen siitä, että Traficomin tehtäviä selkeytettäisiin tietojärjestelmän turvallisuuteen liittyvän turvallisuusjohtamisen (hallinnollinen turvallisuus ja henkilöstöturvallisuus) arvioinnin osalta. Selkeytyksen ei arvioida aiheuttavan Traficomin työmäärään merkittävää lisäystä, ja siten lisäresursointitarpeetkin pysynevät maltillisina.

Fyysiseen turvallisuuteen liittyvien arviointivastuiden selkeyttäminen

Traficom pitää ehdotusta tietoturvallisuuden fyysisen turvallisuuden arvioinnin vastuuviranomaisen selkeästä säätämisestä kannatettavana. Tietoturvallisuus mielletään yleensä rakentuvaksi kolmesta pääpilarista, joita ovat tietojen suojaaminen turvallisuusjohtamisen (sis. hallinnollinen turvallisuus ja henkilöstöturvallisuus), fyysisen turvallisuuden ja teknisen tietoturvallisuuden keinoin. Jos jokin näistä pilareista puuttuu, sähköisessä muodossa (tietojärjestelmissä) olevien tietojen suojaus ei yleensä onnistua luotettavasti. Traficom kannattaa fyysisen turvallisuuden arviointiviranomaisen rooliin viranomaista tai viranomaisia, jolla/joilla on jo valmiiksi syvällinen aihepiirin osaaminen. Tällaisia ovat nykytilassa sekä suojelupoliisi että Puolustusvoimat, jotka kummatkin ovat myös kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) sekä myös turvallisuusselvityslain (726/2014) mukaisia fyysisen turvallisuuden arvioinnin vastuuviranomaisia. Vastuuviranomaiselle/vastuuviranomaisille arvioinneista syntyvä lisätyökuorma tulee luonnollisesti huomioida myös resurssilisäyksinä.

Jatkuvuuteen ja varautumiseen liittyvien arviointivastuiden selkeyttäminen

Traficom näkee perustelluksi muutosehdotuksen siitä, että Traficomin tehtäviä selkeytettäisiin ja laajennettaisiin tietojärjestelmien jatkuvuuden ja varautumisen arvioinnin osalta. Traficom kuitenkin korostaa, että tehtävälisäys edellyttäisi tehtäväkentän rajausten yksityiskohtaista selvitystyötä. Olettaen, että tehtävälisäys kohdistuisi vain tietojärjestelmiin liittyvään jatkuvuuteen ja varautumiseen, tulisi selvittää muun muassa se, kuinka tehtäväkenttä rajautuisi tilanteissa, joissa viranomaisen tietojärjestelmän jatkuvuus tai varautuminen on riippuvainen myös muiden viranomaisten tai/ja kaupallisten toimijoiden tietojärjestelmien ja niitä tukevien järjestelyjen toimivuudesta. Yksinkertaisena esimerkkinä pitkäaikaisen sähkönsyötön varmistaminen, minkä luotettava selvittäminen voi edellyttää arvioinnin laajentamista myös sähköverkon luotettavuuteen. Mikäli tehtävälisäystä ei kohdistettaisi vain tietojärjestelmiin liittyvään jatkuvuuteen ja varautumiseen, tehtäväkenttä voisi laajentua entisestäänkin kyseisen viranomaisen sekä sen sidosryhmien jatkuvuuden ja varautumisen arviointiin. Tehtäväkentän määrityksessä tulisi selvittää myös se, toivotaanko jatkuvuuteen ja varautumiseen liittyvillä arvioinneilla tilannekuvaa esimerkiksi vain tiedon, tietojärjestelmän, kyseisen organisaation tai/ja yhteiskunnan toimivuuden näkökulmista. Riippuen tehtäväkentän rajauksista, laajennetut tehtävät edellyttäisivät Traficomille huomattavia tai merkittäviä lisäresursointitarpeita. On tärkeää, että viranomaisella, jonka tietojärjestelmästä on kysymys, on kokonaiskäsitys ja ymmärrys tietojärjestelmän merkityksestä viranomaisen oman toiminnan jatkuvuuden ja varautumisen kannalta ja myös yhteiskunnan toimivuuden kannalta.

Jatkoselvityksessä tulisi ensin arvioida jatkuvuuteen ja varautumiseen liittyvät lainsäädäntötarpeet, jonka jälkeen olisi mahdollista arvioida lakisääteisten vaatimusten täyttymistä koskevan arviointitoiminnan toteutusmallia ja sen edellyttämiä lainsäädäntömuutostarpeita.

Yksityiset henkilöt arviointitoiminnan apuna

Arviomuistiossa esitetään, että resursoinnin varmistamiseksi arvioinneissa voitaisiin käyttää apuna yksityisiä henkilöitä. Traficom pitää esitettyä mallia tietoturvallisuuden arvioinnin ja turvallisuusluokiteltua tietoa sisältävän jatkuvuuden ja varautumisen arvioinnin osalta ongelmallisena. Yksityisten henkilöiden riittävästä osaamisesta varmistumisesta ja osaamisen ylläpitämisestä aiheutuisi vastaavansuuruinen lisäresurssitarve, kuin henkilöiden toimiminen Traficomin omina virkamiehinä. Traficomin tulisi varmistua myös yksityisten henkilöiden tietojenkäsittelyn turvallisuudesta, mukaan lukien turvallisista toimitiloista varmistuminen, ja yhteensopivuudesta Traficomin oman tietojenkäsittelyn kanssa, mikä pystyttäisiin toteuttamaan kustannustehokkaammin henkilöiden toimiessa Traficomin virkamiehinä. Lisäksi on huomioitava, että yksityisille henkilöille ei erityisesti kansainvälisistä velvoitteista johtuen voitaisi luovuttaa myöskään kaikkea arvioinneissa tarpeellista tietoa, mikä heikentäisi myös yksityisten henkilöiden työn laatua ja tehokkuutta. Traficom näkeekin, että kustannustehokkain ratkaisumalli lisäresursointiin olisi Traficomin arvioijaresurssien suora, vaiheittainen lisääminen uusien tehtävien tuottaman työmäärän toteuman mukaisesti. Muiden olennaisten vaatimusten arvioinnin osalta Traficom katsoo, että malli, jossa hyödynnetään yksityisiä henkilöitä, voi olla hyödynnettävissä.

Puolustusvoimille ehdotettu arvioijarooli

Traficom katsoo, että arviomuistioon kirjattua ehdotusta Puolustusvoimien arvioijaroolista on syytä tarkastella tarpeellisuuden, sekä erityisesti objektiivisuuden ja riippumattomuuden näkökulmasta. Kukin viranomainen voi jo nykysäädännön mukaan arvioida kansallista turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmiensä teknistä tietoturvallisuutta, jatkuvuutta ja varautumista, sekä fyysistä turvallisuutta. Esimerkiksi jo tiedonhallintalain (906/2019) 13 § edellyttää riskien selvittämistä ja tietoturvallisuustoimenpiteiden riskiperustaista mitoittamista, sisältäen esimerkiksi jäännösriskien ja tietojärjestelmien käyttöönottoon liittyvät viranomaisen sisäiset hyväksyntäpäätökset. Viranomaisten tietojärjestelmien osalta Traficom ei näe ehdotetun muutoksen muuttavan nykytilaa, ja ei siten näe sille välttämätöntä tarvetta.

Mahdollinen muutos voisi kuitenkin tukea Puolustusvoimien sisäisen arviointitoiminnallisuuden objektiivisuutta ja riippumattomuutta, mikäli vaatimus riippumattomuudesta ja objektiivisuudesta kirjataan lainsäädäntöön. Erillismaininnat eivät ratkaisisi kuitenkaan toiminnallisiin tarpeisiin ja arviointipäätöksiin liittyvää päätöksentekoristiriitaa tilanteissa, joissa toiminnallisista tarpeista ja arviointipäätöksistä vastaavat toiminnallisuudet kuuluvat saman organisaation komentoketjuun.

Traficom myös suosittelee kiinnitettävän erityishuomiota mahdollisen säännöksen sanamuotoihin ja määritelmiin, sillä esimerkiksi arviomuistion kirjaus "maanpuolustukseen liittyvistä tiedoista" voidaan tulkita monilla eri tavoilla.

Arviomuistioon kirjattuun mainintaan mahdollisesta muutostarpeesta myös turvallisuusselvityslakiin (726/2014) liittyy samansuuntaisia tarkastelutarpeita. Kukin viranomainen voi jo nykysäädännön mukaan arvioida tietojärjestelmiensä tietoturvallisuutta (906/2019, 13 §), ja lisäksi viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle (1101/2019, 6 §). Viranomainen voikin jo nykylainsäädännön keinoin arvioida yrityksille luovuttamiensa tietojen suojauksia kyseisessä yrityksessä. Tästä näkökulmasta Traficom ei näe tarvetta turvallisuusselvityslain muuttamiselle.

Lisäksi on huomioitava, että esimerkiksi ilmaisu "maanpuolustukseen liittyvät tiedot" voisi olla tulkittavissa myös siten, että Puolustusvoimat tekisi käytännössä valtaosan yritysturvallisuusselvitysten tietojärjestelmäarvioinneista. Traficom näkee tämän ongelmalliseksi erityisesti objektiivisuuden ja riippumattomuuden, kansainvälisen yhteensopivuuden sekä myös kustannustehokkuuden näkökulmista.

Yritysturvallisuusselvityksessä tehtävien tietojärjestelmäarviointien sisällön ja tulkintapäätösten tulee olla objektiivisia ja riippumattomia tietojärjestelmässä käsiteltävien turvallisuusluokiteltujen tietojen omistavien viranomaisten mahdollisesti eroavista riskikäsityksistä. Vaikka tietyistä suojauspuutteista johtuvat riskit saattaisivatkin olla yksittäisen tietoon määräämisvallassa olevan viranomaisen sisäisessä riskienhallinnassa hyväksyttävissä esimerkiksi kyseiseen hankkeeseen liittyvien tietojen osalta, yritysturvallisuusselvityksessä tehtävien arviointien tulisi huomioida tietojenkäsittely-ympäristön soveltuvuus myös muiden viranomaisten, mukaan lukien ulkomaan viranomaisten, tietojen käsittelyyn. Tilanne korostuu erityisesti kansainvälisten turvallisuusluokiteltujen tietojen suojaamisessa, missä kansainvälisten turvallisuusluokiteltujen tietojen omistajien tai/ja originaattorien riskinäkemykset ja suojausvaatimukset voivat erota paikoin merkittävästikin siitä, mitä kansalliset asiakasviranomaiset asettavat kansallisiin hankkeisiinsa.

Mikäli eri viranomaisten tekemien hankekohtaisten arviointien ja yritysturvallisuusselvitykseen liittyvien kansallisten tai/ja kansainvälisten arviointien raja hämärtyisi, tällä voisi olla lukuisia ei-toivottuja seurauksia. Yrityksille voisi jäädä epäselväksi esimerkiksi se, onko heidän tietojenkäsittely-ympäristöön kohdistettu arviointi hyväksiluettavissa vain kyseisen viranomaisen tietojen vain kyseiseen hankkeeseen liittyvien tietojen käsittelyyn, myös kyseisen viranomaisen muiden hankkeiden tietojen käsittelyyn, myös muiden viranomaisten kansallisten tietojen käsittelyyn tai/ja myös kansainvälisen turvallisuusluokitellun tiedon käsittelyyn. Eroavaisuudet vaatimuksissa, niiden tulkinnassa tai todentamiskäytännöissä johtaisivat herkästi myös siihen, että yrityksen tietojenkäsittely-ympäristöön jouduttaisiin kohdistamaan erillisarvioinnit kunkin tarpeen näkökulmasta. Tämä voisi aiheuttaa merkittäviä viiveitä ja kustannuksia sekä tietojenkäsittely-ympäristön suunnitteluun ja toteutukseen, että näiden uusimiseen ja uudelleenarviointiin aina kunkin tarpeen näkökulmasta erikseen. Haasteet myös kertautuisivat tilanteissa, joissa yrityksen tietojärjestelmiä olisi tarve liittää osaksi eri viranomaisten tietojärjestelmäkokonaisuuksia.

Lisäksi on huomioitava nykysäädännön vahvuus sekä kansallisten että kansainvälisten tietojärjestelmäarviointien keskittämisessä Traficomille. Keskittämisen kiistämättömiä vahvuuksia ovat esimerkiksi vaatimustulkintojen ja arviointiin käytettyjen todennusmenetelmien yhdenmukaisuus, sekä arviointien suorat hyväksilukemismahdollisuudet sekä kansallisiin että kansainvälisiin tarpeisiin. Traficom korostaakin, että arviointitoimintaan liittyvän kyvykkyyden rakentamisessa ja ylläpidossa merkittävässä asemassa on menetelmien yhteensopivuus ja vastaavuus kansainvälisten organisaatioiden ja niiden jäsenmaiden käyttämien menetelmien kanssa. Tietojärjestelmien suojausten tulisi kestää myös sellaiset hyökkäysmenetelmät, joista Suomi ei ilman kansainvälistä yhteistyötä saisi tietoa. Traficomin Kyberturvallisuuskeskuksen kyvykkyyden rakentamisessa ja ylläpidossa merkittävässä asemassa onkin ollut Kyberturvallisuuskeskuksen kansainvälisiltä viranomaisyhteistyökumppaneilta saadut parhaat käytännöt ja osin myös yhteinen kehitystyö. Tämä mahdollistaa jatkossakin edistyksellisen, erinomaisesti myös kansainvälistä vertailua kestävän kyvykkyyden ylläpitämisen Suomen kaltaisessa, rajatuin resurssein toimivassa maassa. Traficomin Kyberturvallisuuskeskus tuottaa myös kyberturvallisuuden tilannekuvaa, jonka merkitys tietojärjestelmien riskiarvioinneissa on huomattava.

Nykysäädännön mukainen menettely on osoittautunut myös hyvin kustannustehokkaaksi erityisesti tilanteissa, joissa alun perin vain kansallisiin tarpeisiin tehty tietojärjestelmäarviointi on pystytty laajentamaan kattamaan myös kansainväliset tarpeet. Mikäli yritysturvallisuusselvitysten tietojärjestelmäarvioinnit hajautettaisiin useammalle viranomaiselle, keskittämisestä kiistämättömästi saatavat edut menetettäisiin osin tai pahimmillaan jopa kokonaan. Esimerkiksi tilanteessa, jossa toisen viranomaisen arvioiman yrityksen tietojärjestelmäkokonaisuus haluttaisiin laajentaa kattamaan myös kansainvälisen turvallisuusluokitellun tiedon suojaamisen, joutuisi Traficom pahimmillaan arvioimaan koko tietojärjestelmäkokonaisuuden uudestaan. Tällä olisi päällekkäisen työn lisäksi myös selkeitä aikataulu- ja kustannusvaikutuksia, mikä heikentäisi myös suomalaisen yrityskentän mahdollisuuksia päästä mukaan esimerkiksi kansainvälisiin tarjouskilpailuihin.

Arviointilaitosten hyväksyntään ja valvontaan ehdotetut muutokset

Traficom näkee perustelluksi arviomuistiossa esitetyn yleisperiaatteen siitä, että arviointilaitoksia koskevaan lakiin tehtäisiin vain välttämättömiä päivityksiä ja sen kokonaisuudistus jäisi myöhemmin muun muassa EU:n kyberturvallisuusasetuksen ja tietosuoja-asetuksen perusteella kehittyvien sertifiointimekanismien perusteella tehtävän uudelleenarvioinnin varaan.

Arviomuistiossa toisaalta ehdotetaan, että arviointilaitoslakia tulisi muuttaa siten, että siinä asetetaan sekä arviointilaitokselle että sen palveluksessa olevalle arvioitsijalle yksilöidyt vaatimukset, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa. Traficom näkee perusteltuna sen, että arviointilaitokselle asetettavat vaatimukset kuvataan nykyistä yksityiskohtaisemmin myös lakitasoisina. Kuvauksien tulee kuitenkin olla aikaa kestäviä, jotta ne eivät menetä merkitystään nopeasti etenevän tietojärjestelmiin liittyvän teknisen kehityksen myötä. Lakitasoisten vaatimusten tueksi tarvitaan nykytilan mukaisesti myös täsmälliset, yksikäsitteiset vaatimustulkinnat kullekin lakisääteiselle vaatimukselle. Esimerkiksi riittävä pätevyysaluekohtainen todennusosaaminen tulisi jatkossa olla nostettuna myös lakitasoiseksi vaatimukseksi, ja sen tulkinta tulisi pitää nykymallin mukaisesti ohjetasoisena. Tällainen lähestymistapa nostaisi keskeiset vaatimukset lakitasoisiksi ja siten suoraviivaisemmin valvottaviksi, mutta kestäisi kuitenkin paremmin aikaa mahdollistaen esimerkiksi uusien teknologioiden huomioinnin ohjetason päivitysten piirissä.

Traficom näkee perustelluksi arvioitsijoille asetettavien vaatimusten taustan erityisesti siitä näkökulmasta, että arviointilaitosten henkilövaihdokset tulisi saada nykyistä selvemmin arviointilaitoksiin kohdistuvan valvonnan kohteeksi. Tämä mahdollistaisi nykyistä tehokkaammin myös arviointilaitoksen hyväksynnän rajaamisen tai perumisen tilanteissa, joissa arviointilaitoksella ei henkilövaihdosten takia ole enää tosiasiallisesti käytettävissään arviointilaitostoiminnan edellyttämää osaamista. Traficom näkee sen sijaan arvioitsijoille laajemmin asetettavien vaatimusten johtavan mahdollisesti ei-toivottuun lopputulokseen. Luotettava tietojärjestelmien arviointitoiminta edellyttää monipuolisten todennusmenetelmien osaamista ja eri todennusmenetelmien tuottamien tulosten ristiinvertailua luotettavan arviointituloksen varmistamiseksi. Keskeisimmät arvioinneissa käytetyt hallinnolliset todennusmenetelmät sisältävät henkilöstöhaastattelut (H1) ja dokumentaatioon tutustumisen (H2). Keskeisimmät tekniset todennusmenetelmät sisältävät puolestaan passiivisen rajapinta-analyysin (T1), aktiivisen rajapinta-analyysin (T3), järjestelmäkonfiguraatioiden turvallisuuden tarkastelun (T2), sovellusturvallisuuden tarkastelun järjestelmätyypeittäin (T4), salausratkaisujen turvallisuuden todentamisen (T5), käytettävyystestaukset (ml. kuormitustestaukset) (T6), fyysisen turvallisuuden suojausten todentamismenetelmät (T7), yhdyskäytäväratkaisujen turvallisuuden testaukset (T8), poikkeamahavainnointikyvyn testaukset (T9), hajasäteilysuojausten todentamisen (T10) sekä luvattomien teknisten laitteiden olemassaolon todentamisen (T11). Kaikkien todennusmenetelmien ja teknologioiden syvällinen osaaminen ei ole realistista yksittäiselle arvioijalle. Hallinnollisen ja teknisen yleisen todennusosaamisen ja yleisten teknologioiden lisäksi arvioijat syventyvät ja erikoistuvat tyypillisesti vain yksittäisiin erikoistumisalueisiin. Luotettavaan arviointiin kykenevän arvioijaryhmän valinnassa tuleekin aina huomioida turvallisuuteen vaikuttavan kokonaisuuden ymmärrys, sekä lisäksi pystyä tunnistamaan kyseisen kohteen arvioinnissa tarvittava erikoisosaaminen, ja sisällyttää arvioijaryhmään myös tällaisen omaavat asiantuntijat. Sen sijaan kaikkien erikoistumisalueiden syvällisen osaamisen edellyttäminen yksittäisiltä arvioijilta voisi johtaa joko todennusosaamiselta edellytettävän syvällisyyden karsiutumiseen, heikentäen arviointien luotettavuutta, tai siihen, että arviointilaitosten pätevyysalueiden hyväksynnät raukeaisivat hyväksyttyjen arvioijien puutteesta johtuen. Yksittäisille arvioijille asetettavat vaatimukset voisivat kattaa sen sijaan hallinnollisen ja teknisen yleisen todennusosaamisen ja turvallisuuteen vaikuttavan kokonaisuuden ymmärryksen lisäksi yksittäisiä erikoistumisalueita.

Traficom myös huomauttaa, että arviomuistiossa esitetty näkemys siitä, että arvioinnin tekijän kelpoisuutta ei voida kohdentaa pelkästään yleisesti organisaatioon, vaan myös tosiasiassa arviointeja tekeviin henkilöihin, sekä johtopäätös siitä, että siten myös arvioitsijoille tulisi asettaa lakitasoiset pätevyysvaatimukset, vaikuttaisi perustuvan osin puutteelliseen kuvaan nykytilasta. Traficom näkeekin, että osaamisen arvioinnissa tulisi jatkossakin keskittyä arviointilaitoksen

kyvykkyyteen kasata pätevä arvioijaryhmä, jossa turvallisuuden kokonaisuuden ymmärryksen lisäksi ryhmän jäsenten erityisosaaminen kattaa kokonaisuudessaan kyseisessä arvioinnissa tarvittavan osaamisen. Arviointilaitoksella tulisi toisin sanoen jatkossakin olla keskeisten osaamisalueiden osalta riittävä osaaminen eri henkilöiden osaamista yhdistelemällä, sekä kyvykkyys kuhunkin arviointikohteeseen riittävän pätevän arvioijaryhmän kokoamiseen. Nykymenettelyä voitaisiin kuitenkin täydentää arvioijakohtaisilla vaatimuksilla. Tällainen lähestymistapa jättäisi myös arviointilaitoksille enemmän liikkumavaraa toimintansa järjestämiseen, mikä tukee suoraan myös arviomuistiossa esitettyä tavoitetta arviointilaitosten määrän lisäämiselle.

Traficom nostaa myös esille, että ehdotettu yksittäisten arvioitsijoiden pätevyyden arviointi, arviointiryhmän yhdistetyn osaamisen sijaan, edellyttäisi uuden arvioijapätevyyden testaus- ja valvontajärjestelmän luontia nykyisen arviointilaitosten akkreditointi- ja hyväksyntämenettelyn täydennykseksi. Kuten edellä jo kuvattu, kaikkien todennusmenetelmien ja teknologioiden syvällinen osaaminen ei ole realistista yksittäiselle arvioijalle, jolloin myös henkilötason testaus- ja valvontajärjestelmän tulisi kattaa erilaisia arvioijarooleja. Traficom näkee tällaisen järjestelmän laadinnan, käyttöönoton, ylläpidon ja valvonnan mahdollisena, mutta korostaa sen edellyttävän lisäresursointia. Traficom kuitenkin huomauttaa, että uuden järjestelmän käyttöönoton on vaikea nähdä tukevan arviomuistion tavoitetta arviointilaitosten markkinoille pääsyn nopeuttamisesta.

Traficom myös korostaa, että jo nykytilanteen haasteena on se, että arviointilaitosten osaaminen ei kaikilta osin vastaa viranomaisarvioinnin edellytyksiä, ja arviointilaitosten pätevyysalueita on jouduttu hyväksymään osittaisina. Arviointilaitosten pätevyysalueet eivät kata esimerkiksi salausratkaisujen, yhdyskäytäväratkaisujen tai hajasäteilysuojausten riittävyyden arviointia kuin osittaisina ja rajauksin. Huomioitavaa onkin, että kaupallisesti ei ole saatavilla riittävän kattavia koulutus- ja pätevöittämisohjelmia arvioitsijoilta edellytettävään osaamiseen. Traficom toteaa esimerkkinä, että kaupallisesti saatavilla olevat koulutukset ja erilaiset sertifioinnit eivät kata Traficomin Kyberturvallisuuskeskuksen arviointitoiminnalta edellytettyä osaamista kuin osittain. Kyberturvallisuuskeskus joutuukin siten itse kouluttamaan henkilöstöään vain viranomaiskentässä käytössä oleviin arviointimenetelmiin. Tietojärjestelmäarvioijien sisäistä koulutuskokonaisuutta on kehitetty pitkäjänteisesti koko arviointitoiminnan yli kymmenen vuoden olemassa olon ajan. Uusille tietojärjestelmäarvioijille on Kyberturvallisuuskeskuksessa käytössä muun muassa kahden vuoden koulutusohjelma, johon sisältyy yli 200 koulutusosiota. Kyberturvallisuuskeskuksen sisäistä tietojärjestelmäarvioitsijoiden koulutus- ja pätevöittämisohjelmaa ei voida sellaisenaan kuitenkaan laajentaa viranomaiskentän ulkopuolelle sen sisältämien, vain Kyberturvallisuuskeskuksen käyttöön luovutettujen turvallisuusluokiteltujen tietojen vuoksi. Arviomuistiossa kuvattu ehdotus arvioijille asetettavista vaatimuksista edellyttäisikin testaus- ja valvontajärjestelmän lisäksi jatkotarkastelua myös siitä, kuinka arviointilaitosten henkilöstön riittävän laaja-alainen ja toisaalta riittävän syvällinen koulutus voitaisiin toteuttaa kustannustehokkaasti.

Traficom näkee ehdotuksen yritysturvallisuusselvityksen hyödyntämisestä arviointilaitosten tietojenkäsittelyn turvallisuuden arvioinnissa erittäin perusteltuna. Yritysturvallisuusselvityksen hyödyntäminen mahdollistaa osin päällekkäisen viranomaisrakenteen purkamisen arviointilaitoksen tietojenkäsittelyn turvallisuudesta varmistumisessa. Osittaiselle päällekkäisyydelle ei ole enää tarvetta, sillä vastaavat mekanismit sisältyvät jo arviointilaitoslain jälkeen voimaan astuneen turvallisuusselvityslain mukaiseen yritysturvallisuusselvitykseen. Yritysturvallisuusselvityksen hyödyntäminen tukisi nykyistä kattavammin myös ulkomaiseen omistukseen ja vaikutusvaltaan (FOCI, Foreign Ownership, Control or Influence) liittyvien riskien huomiointia. Traficom arvioi, että yritysturvallisuusselvityksen hyödyntäminen turvallisuusluokiteltua tietoa käsittelevien arviointilaitosten hyväksyntäprosessissa ei edellyttäisi muutoksia turvallisuusselvityslakiin, vaan

pystyttäisiin toteuttamaan pienillä muutoksilla nykyisen arviointilaitoslain kirjauksiin. Traficom pitää tärkeänä, että yritysturvallisuusselvitystä voitaisiin hyödyntää arviointilaitosten tietoturvallisuuden varmistamisessa mahdollisimman pian.

Traficom ei sen sijaan näe perusteltuna arviointilaitosten hyväksyntä- tai valvontavastuun siirtämistä Traficomilta FINAS:ille. Nykymallin mukainen Traficomin ja FINAS:in välinen työnjako on selkeä ja rajallisten viranomaisresurssien käyttö on saatu nykymallissa hyödynnettyä tehokkaasti. Tietojenkäsittelyn turvallisuuden lisäksi Traficom arvioi nykymallissa arviointilaitosten sisäisen ohjeistuksen asianmukaisuutta arviointilaitoksen toiminnan ja sen seurantaa varten, millä on suora kytkös myös arviointilaitoksen käytännön toimintaan ja sen valvontaan. Arviointilaitosten valvonta on osoittautunut välttämättömäksi mekanismiksi arviointilaitosten työn laadun varmistamisessa ja havaittujen puutteiden korjauttamisessa. Arviointilaitosten valvontatoiminta edellyttää rajallisesti saatavilla olevan erityisosaamisen lisäksi myös turvallisuusluokan II mukaista tietojenkäsittely-ympäristöä, joka Traficomilla on jo valmiina. Muutokset vastuisiin edellyttäisivätkin erittäin merkittävää lisäresursointia. Traficom ehdottaa sen sijaan, että kansalliseen turvallisuuteen liittyvien pätevyysalueiden ulkopuolisten pätevyysalueiden valvontaan osallistuisivat jatkossa kyseisen pätevyysalueen vastuuviranomaiset, esimerkkeinä toisiolain (552/2019) mukaisten arviointien osalta Valvira ja tietosuojaan liittyvien kokonaisuuksien osalta tietosuojavaltuutettu.

Traficom ei kannata arviomuistiossa ehdotettua vaihtoehtoista mallia siitä, että viranomaisiin kohdistuvasta arviointilaitosjärjestelmästä luovuttaisiin. Kuten edellä jo todettu, tämä edellyttäisi merkittävää lisäresursointitarvetta Traficomille, minkä ratkaisemiseksi ehdotettu malli yksityisten arvioijien käytöstä päinvastoin lisäisi resursointitarvetta sekä arvioijien osaamisesta varmistumiseen, jatkuvaan kouluttamiseen, valvontaan, sekä arvioinnissa välttämättömien luotettavien tietojenkäsittely-ympäristöjen ja toimitilojen tarjoamiseen yksityisille arvioijille. Lainsäädännön muutoksissa tulee ottaa huomioon myös liiketoiminnan jatkuvuutta koskevat näkökulmat.

Vaatimustenmukaisuuden osoittamiseen liittyvät muutosehdotukset

Traficom pitää perusteltuna, että tietojärjestelmien arviointeja hyödynnettäisiin nykyistä laajemmin osana viranomaisten riskienhallintatyötä. Arviointien laajempi hyödyntäminen tukisikin suoraan tiedonhallintalain 13 §:ssä viranomaiselta edellytettävää riskien selvittämistä ja tietoturvallisuustoimenpiteiden riskiperustaista mitoittamista. Traficom pitää perusteltuna myös sitä, että viranomaisen määrittämiin kriittisimpiin tietojärjestelmiin kohdistettaisiin riippumaton, ulkopuolinen arviointi, jonka tulokset olisivat siten suoraan hyödynnettävissä viranomaisen riskienhallintatyössä.

Traficom ei sen sijaan näe perusteltuna arviomuistion ehdotusta todistusten edellyttämisen laajentamisesta. Arviomuistiossa esitetty ehdotuksen perustelu, yhteisten tieto- ja viestintäteknisten palvelujen arviointiraporttien hyödyntämishaasteet, viittaa oireen eikä taudin hoitamiseen. Traficom suosittelee sen sijaan sitä, että yhteisten tieto- ja viestintäteknisten palvelujen suojaukset tulisi toteuttaa riittävän luotettavina, ja että palvelutuottajia edellytettäisiin toimittamaan raportit palvelujen käytöstä päättävien viranomaisten tiedonhallintayksiköiden riskienhallintatyön tueksi.

Kriteeristöihin liittyvät muutosehdotukset

Traficom näkee perusteltuna, että arviointikriteeristöjä kehitetään ja räätälöidään erilaisiin käyttötapauksiin, säästäen viranomaisilta räätälöintiin muuten kuluvaa työmäärää. Traficom näkee erityisen kannatettavana sen, että arviointikriteeristöjen kehitystyö keskitetään nykykriteeristöjen katvealueisiin, erityisesti julkisen tiedon, turvallisuusluokittelemattoman salassa pidettävän tiedon, toiminnan jatkuvuuteen ja varautumiseen, sekä myös henkilötietojen suojaamiseen liittyen. Traficom pitää erittäin perusteltuna myös sitä, että pyörää ei pyritä keksimään uudelleen, vaan että uusissa kriteeristöissä hyödynnetään jo tehtyä laadukasta työtä. Esimerkiksi tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5) ja Katakri 2020 -arviointityökalu valmisteltiin 2020 aikana rinnakkain, kansallisen turvallisuusluokitellun tiedon suojaamisen näkökulmasta, ja kattavat yhtenäisessä muodossa keskeiset kansallisen turvallisuusluokitellun tiedon suojaamiseen liittyvät näkökulmat. Hyödyntämällä edellä mainittuja kansallisen turvallisuusluokitellun tiedon suojaamiseen jatkossakin, kriteeristötyössä on samalla mahdollisuus saavuttaa yhteensopivuus ja suora hyödynnettävyys myös turvallisuusselvityslain (726/2014) mukaisissa yritysturvallisuusselvityksissä tehtyjen ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) mukaan tehtyjen arviointien kanssa.

Traficom nostaa huomiona kuitenkin esille, että osa arviomuistion kriteeristöihin liittyvistä kirjauksista vaikuttaisi perustuvan osin puutteelliseen nykytilakuvaan. Esimerkiksi Katakri 2020:n roolista olisi hyvä huomioida, että se ei itsessään aseta vaatimuksia, vaan on laadittu työkaluksi lainsäädännössä olevien vaatimusten täyttymisen arviointiin.

Traficom pitää perusteltuna myös arviomuistion kirjausta siitä, että riskienhallinnan rooli huomioidaan asetettavissa vaatimuksissa. Traficom kuitenkin korostaa, että tietojärjestelmän tai palvelun arvioinnissa tulee huomioida tiedonhallintayksikön ja ulkopuolisen riippumattoman riskienarvioinnin eroavat roolit ja perusteet. Tiedonhallintayksikön riskienarvioinnissa korostuu viranomaisen toiminnan erityispiirteiden huomiointi. Ulkopuolisen riippumattoman arvioinnin roolina on puolestaan arvioida suojauksia tiedonkäsittelyyn kohdistuvia yleisiä riskejä vastaan. Arvioinnin käyttötapausten kuvauksissa tuleekin selkeästi tuoda tämä eroavaisuus esille, sekä huomioida myös se, että vaikka jokin toteutus olisi tiedonhallintayksikön riskienarvioinnissa hyväksyttävissä, se saattaa silti olla riittämätön yleisiin riskeihin nähden ja siten näyttäytyä ulkopuolisen arvioinnin raportissa poikkeamana.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

-

10. Muut yleiset kommentit arviomuistiosta

-

Pahlman Sauli
Traficom

Erkkilä Johanna
Liikenne- ja viestintävirasto - Kyberturvallisuuskeskus