VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Asettamispäätös

16.2.2024

VN/36127/2023
VN/36127/2023-VM-2

VM: Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän asettaminen

Toimikausi

Julkisen hallinnon tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän toimikausi on 1.3.2024 – 31.12.2025.

Tausta

Tietojärjestelmien vaatimustenmukaisuuden arviointia koskeva EU-sääntely on viime vuosina lisääntynyt. Samalla digitalisaation edistyminen ja kehittyvät teknologiat kuten pilvipalvelut, tekoäly ja kvanttilaskenta ovat vaikuttamassa sekä toimintatapoihin että menettelyihin toteuttaa julkisen hallinnon tietojärjestelmiä. Julkisen hallinnon tietojärjestelmien ja yhteisten palveluiden vaatimustenmukaisuuden arvioinnin keskeinen sääntely: laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1046/2011, arviointilaki) sekä laki tietoturvallisuuden arviointilaitoksista (1045/2011, arviointilaitoslaki) (jatkossa yhdessä arviointilait) on valmisteltu yli 12 vuotta sitten. Keskeistä arviointeihin liittyvää kansallista sääntelyä kuten laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) sekä turvallisuusselvityslaki (726/2014) on valmistunut arviointilakien jälkeen.

Julkisen hallinnon tietojärjestelmiin ja yhteisiin palveluihin voi kohdistua arviointitarpeita myös kansainvälisten tietoturvallisuusvelvoitteiden johdosta. EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskee laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki). Yhtenä haasteena nähdään kansallisen ja kansainvälisen toiminnan, tietojärjestelmien ja yhteisten palveluiden saattaminen vastaamaan Nato-vaatimuksia.

Julkisen hallinnon tietojärjestelmien vaatimustenmukaisuuden arviointitarpeita ovat myös kasvattaneet turvallisuusympäristön muutokset ja siihen liittyvä teknologioiden ja tiedonhallinnan rooli geopoliittisessa kilpailussa, yhä kehittyneemmät uhkat, verkottuneemmat järjestelmät ja monimutkaisemmat logistiset toimitusketjut sekä uhkilta suojautumisen kehittyminen, tiedon salaamisen merkityksen kasvaminen osana tiedon elinkaarta ja käsittelyä ja ICT-järjestelmien kustannustason nousu suhteessa muuhun kulurakenteeseen.

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Valtiovarainministeriö PL 28 00023 Valtioneuvosto	Snellmaninkatu 1 A Helsinki	0295 16001 +358 295 16001		kirjaamo.vm@gov.fi

Arviointien ja sertifiointien automatisointimahdollisuuksia tutkitaan. Esimerkiksi mahdollisuudet tulevaisuudessa ylläpitää sertifikaattia automaattiseen sertifiointiratkaisuun perustuen vaikuttavat lupaavilta. Myös arviointilakien ja arviointien mahdollisia uudistamistarpeita koskeneet viime vuosina tehdyt selvitykset puoltavat niiden ajantasaistamista ja tehostamista.

EU- ja kansallisen sääntelyn, kansainvälisen ja kansallisen toimintaympäristön ja turvallisuustilanteen muutosten sekä teknologioiden kehittymisen ja tehtyjen selvitysten perusteella julkisen hallinnon tietojärjestelmien ja yhteisten palveluiden sekä niiden hyödyntämisen jatkuvuuden ja varautumisen vaatimustenmukaisuuden arvioinnin ajantasaistaminen ja tehostaminen ovat välttämättömiä.

Työryhmän työssä tunnistettavia asiakokonaisuuksia ovat:

- Julkista ja luokittelematonta salassa pidettävää tietoa käsittelevien tietojärjestelmien sekä niiden hyödyntämisen jatkuvuuden ja varautumisen arviointimenettely, mukaan lukien arviointeja tilaavat ja toteuttavat toimijat.

- Turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien sekä niiden hyödyntämisen jatkuvuuden ja varautumisen arviointimenettely, mukaan lukien arviointeja tilaavat ja toteuttavat toimijat.

- Arviointeja toteuttavien toimijoiden ohjaus ja valvonta, eri viranomaisten työnjako sekä hyväksymismenettelyn kehittäminen ja tehostaminen samalla säilyttäen arviointien laadukkuus.

- Voimassa oleva ja valmisteilla oleva tietojärjestelmien vaatimustenmukaisuuden arviointiin liittyvä EU-lainsäädäntö; missä määrin se vaikuttaa mahdollisuuksiin asettaa kansallisissa säädöksissä arviointivaatimuksia ja kehittää kansallista arviointijärjestelmää. Yksi keskeinen näkökulma on kyberturvallisuusasetuksen (CSA) mukaisen sertifiointijärjestelmän kattaman alan laajuus.

- Tietojärjestelmien vaatimustenmukaisuuden arviointia koskeva sääntely ja käytäntö valituissa EU-vertailumaissa, mukaan lukien mahdolliset kyberturvallisuusasetuksesta (CSA) johtuvat muutostarpeet sääntelyyn valituissa vertailumaissa.

- Sääntelyn kokonaisuus myös arviointiyritystoiminnan näkökulmasta, jotta Suomeen muodostuisi selkeä, kokonaisuuden huomioiva yhteinen raami eri EU-sääntelyiden käsittämälle julkisen hallinnon tietojärjestelmien ja yhteisten palveluiden arviointitoiminnalle.

Tavoite/tehtävä

Työryhmän tavoitteena on hakea kustannustehokkaampia menettelyjä vastata julkisen hallinnon tietojärjestelmien ja yhteisten palveluiden sekä niiden hyödyntämisen jatkuvuuden ja varautumisen arviointitarpeiden kasvuun sekä arvioida nykyisen arviointilainsäädännön ajantasaistamistarpeet ja arviointien tehostamiskeinot.

Työryhmän tehtävänä on valmistella arviointien toteuttajille asetettavat velvoitteet sekä EU:n arviointeja koskevan sääntelyn soveltamisalaan kuulumattomien julkisen hallinnon tietojärjestelmien ja yhteisten palvelujen sekä niiden hyödyntämisen jatkuvuuden ja varautumisen arviointia koskevat velvoitteet.

Arviointien mahdollisia toteuttajia ovat nykytilassa arviointeja toteuttavat liikenne- ja viestintävirasto sekä liikenne- ja viestintäviraston hyväksymät yksityiset arviointilaitokset sekä uutena mahdollisesti myös muiden viranomaisten kuten Puolustusvoimien ja Valtorin riippumattomat arviointiyksiköt. EU:n arviointeja koskevan sääntelyn ulkopuolisia julkisen hallinnon tietojärjestelmiä ja yhteisiä palveluita on käytössä kansallisen turvallisuuden viranomaisilla ja paikallishallinnossa. Velvoitteiden ajantasaistamisessa painotetaan arviointien toteuttamista nykyistä kustannustehokkaammin.

Työryhmän tehtävät jaetaan kahteen vaiheeseen. Ensimmäisessä vaiheessa vuoden 2024 aikana työryhmän tehtävän mukaisen säädösvalmistelun kohteet tunnistetaan ja niihin liittyvät säädösmuutostarpeet arvioidaan, tarkennetaan ja priorisoidaan itsearviointien hyödyntämisen tarjoamat mahdollisuudet, kustannustehokkuus ja toimintaympäristön muutokset huomioiden. Ensimmäisen vaiheen lopputuloksena syntyy raportti, joka on pohjana toisessa vaiheessa toteutettavalle tarkemmalle säädösvalmistelulle.

Työryhmän tehtävien toisessa vaiheessa vuoden 2025 loppuun mennessä tavoitteena on valmistella hallituksen esityksen muotoon ehdotukset tietojärjestelmien ja yhteisten palveluiden vaatimustenmukaisuuden arviointia koskevan lainsäädännön ajantasaistamiseksi. Työryhmän työn valmistuttua arvioidaan erikseen, minkä ministeriön tai ministeriöiden toimialaan ehdotetut säädösmuutokset kuuluvat.

Organisointi

Ryhmän puheenjohtajana toimii tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä. Ryhmän jäsenet ovat:

- neuvotteleva virkamies Mika Kuronen, valtiovarainministeriö, varapuheenjohtaja
- toimialajohtaja Max Hamberg, valtioneuvoston kanslia
  varajäsen johtava asiantuntija Jan Seuri
- tietoturvatarkastaja Mika Pullinen, ulkoministeriö
- johtava asiantuntija Kimmo Janhunen, oikeusministeriö
- turvallisuuspäällikkö Kari Santalahti, sisäministeriö
  varajäsen johtava asiantuntija Ismo Parviainen
- neuvotteleva virkamies Jukka-Pekka Virtanen, puolustusministeriö
- johtava tietohallintoasiantuntija Mika Tuikkanen, maa- ja metsätalousministeriö
  varajäsen erityisasiantuntija Hanna Majurinen
  2. varajäsen erityisasiantuntija Ari Mannonen
- valtion kyberturvallisuusjohtaja Rauli Paananen, liikenne- ja viestintäministeriö
- erityisasiantuntija Lars Dolk, liikenne- ja viestintäministeriö
- erityisasiantuntija Teemu-pekka Virtanen, sosiaali- ja terveysministeriö
- johtava asiantuntija Tanja Karvonen, työ- ja elinkeinoministeriö
  varajäsen erityisasiantuntija Kimmo Kuusela
- IT-erityisasiantuntija Lauri Karppinen, Tietosuojavaltuutetun toimisto
- yksikönpäällikkö Sonja Marjamäki-Ruuskanen, Valtion tieto- ja viestintätekniikkakeskus Valtori
  varajäsen ryhmäpäällikkö Mika Raappana
  2. varajäsen Jyrki Siivola

- erityisasiantuntija Riina Seulasaari, Digi- ja väestötietovirasto
- johtava asiantuntija Anne Lohtander, Liikenne- ja viestintävirasto
- osastoinsinööri Tuomas Munnukka, Puolustusvoimat
  varajäsen everstiluutnantti Kimmo Tarvainen
- erityisasiantuntija Hanna Menna, Hyvil Oy
  varajäsen erityisasiantuntija Marjo Orava
- erityisasiantuntija Martti Setälä, Kuntaliitto

Ryhmän sihteeristössä toimivat tietohallintoneuvos Tuija Kuusisto, neuvotteleva virkamies Mika Kuronen ja hankeassistentti Eeli Pakkala valtiovarainministeriöstä, erityisasiantuntija Lars Dolk liikenne- ja viestintäministeriöstä, hallitussihteeri Tuomas Hyvärinen puolustusministeriöstä, erityisasiantuntija Anna-Minna Lukala ja varajäsen erityisasiantuntija Ella Karvonen sisäministeriöstä, lakimies Jussi Rissanen Liikenne- ja viestintävirastosta, tekninen tietoturvajohtaja Pasi Koljonen ja varajäsen tietoturvajohtaja Timo Kaartosalmi Puolustusvoimista, yksikönpäällikkö Sonja Marjamäki-Ruuskanen ja varajäsen ryhmäpäällikkö Mika Raappana Valtorista ja erityisasiantuntija Hanna Heikkinen Digi- ja väestötietovirastosta.

Työryhmä voi kokouksessaan todeta mahdolliset muutokset jäsentensä osalta.

Kunta- ja alueministeri Anna-Kaisa Ikonen

Budjettineuvos Tomi Hytönen
yksikön päällikkö

Liite Julkisen hallinnon tietojärjestelmien arvioinnin ajantasaistamisen ja tehostamisen tausta

Jakelu
PLM Puolustusministeriö
YM Ympäristöministeriö
OM Oikeusministeriö
UM Ulkoministeriö
Valtion tieto- ja viestintätekniikkakeskus Valtori
Tietosuojavaltuutetun toimisto
Suojelupoliisi
Puolustusvoimat
VNK Valtioneuvoston kanslia
TEM Työ- ja elinkeinoministeriö
LVM Liikenne- ja viestintäministeriö
STM Sosiaali- ja terveysministeriö
Digi- ja väestötietovirasto
OKM Opetus- ja kulttuuriministeriö
MMM Maa- ja metsätalousministeriö
SM Sisäministeriö
UM NSA-00 Kansallinen turvallisuusviranomainen
Hyvinvointialueyhtiö Hyvil Oy
Kuntaliitto

Tiedoksi VM Valtiovarainministeriö

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Liite

16.2.2024

VN/36127/2023
VN/36127/2023-VM-2

Liite: Julkisen hallinnon tietojärjestelmien arvioinnin ajantasaistamisen ja tehostamisen tausta

Tuottavuus

Arviointilakien ajantasaistamisen voidaan arvioida myös lisäävän tuottavuutta julkisen hallinnon tietojärjestelmien elinkaarikustannusten kasvun hillitsemisen ja häiriönsietokyvyn parantumisen kautta. Tietojärjestelmän elinkaaren alusta lähtien toteutettavan säännöllisen vaatimustenmukaisuuden täyttymisen arviointien ja sertifiointien arvioidaan vähentävän järjestelmän elinkaarikustannuksia. Häiriösietokyvyn parantumisella tavoitellaan nopeampaa ja parempaa toipumista erilaisista tietoturvaloukkaustilanteista ja mahdollisten tietovuotojen sekä aineellisten ja aineettomien omaisuuksien menetysten minimoimista. Toimintaympäristön muutosten johdosta on vaatimustenmukaisuuden arvioinnin lisäksi esille noussut kasvava tarve arvioida tietojärjestelmien ja tiedon elinkaaren aikaista kyberresilienssiä ja mahdollisuuksia puolustaa tietojärjestelmiä ja tietoa tietoturvaloukkauksia ja –hyökkäyksiä vastaan.

EU-sääntely

Arviointilakien ajantasaistamisessa huomioitavaa EU-sääntelyä ovat seuraavat:

- Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus, CSA). CSA:n mukaisessa sääntelyjärjestelmässä laaditaan sertifiointiskeemoja, joiden mukaisia arviointeja voivat tehdä akkreditoidut vaatimuksenmukaisuuden arviointilaitokset. Liikenne- ja viestintäviraston tehtävänä on sähköisen viestinnän palveluista annetun lain mukaan (917/2014) 304 §:n 14 kohdan mukaan toimia kyberturvallisuusasetuksen mukaisena kansallisena kyberturvallisuussertifioinnin viranomaisena. Kyberturvallisuusasetuksen 57 artiklan 2 kohdan mukaan jäsenvaltiot eivät saa ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille, jotka kuuluvat jo jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.

- Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS2 -direktiivi). NIS2-direktiivi on luonteeltaan vähimmäisharmonisoiva, eli se ei estä jäsenvaltioita ottamasta käyttöön menettelyitä, joilla varmistetaan kyberturvallisuuden korkeampi taso soveltamisalaan kuuluville toimijoille. NIS2-direktiivin kansallisen täytäntöönpanon säädösehdotusten lausuntokierros on päättynyt. Tiedonhallintalaissa ehdotetaan säädettäväksi tarkastuksessa avustavan tehtävän antamisesta

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Valtiovarainministeriö PL 28 00023 Valtioneuvosto	 Snellmaninkatu 1 A Helsinki	 0295 16001 +358 295 16001		 kirjaamo.vm@gov.fi

hyväksytylle arviointilaitokselle ja arvioinnin teettämisestä hyväksytyllä arviointilaitok-sella. NIS2-direktiivin täytäntöönpanosta on ehdotettu säädettävän myös kyberturvallisuuden riskienhallinnasta annettavassa laissa.

- NIS2-direktiivin 24 artiklassa säädetään eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytöstä niin, että tiettyjen 21 artiklan kyberturvallisuutta koskevien vaatimusten noudattamisen osoittamiseksi jäsenvaltiot voivat vaatia keskeisiä ja tärkeitä toimijoita käyttämään määrättyjä, keskeisen tai tärkeän toimijan itse kehittämiä tai kolmansilta osapuolilta hankittavia TVT-tuotteita, TVT-palveluja ja TVT-prosesseja, jotka on sertifioitu kyberturvallisuusasetuksen (CSA) 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Jäsenvaltioiden on myös kannustettava keskeisiä ja tärkeitä toimijoita käyttämään hyväksyttyjä luottamuspalveluja.

- Lisäksi artiklassa 24 siirretään komissiolle valta antaa delegoituja säädöksiä, joilla täydennetään NIS2-direktiiviä täsmentämällä, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi kyberturvallisuusasetuksen (CSA) 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti.

- Rajat ylittävää sähköistä tunnistamista ja sähköisiä luottamuspalveluja koskevaa EU:n eIDAS-asetusta ((EU) No 910/2014) ollaan parhaillaan muuttamassa.
  - Työryhmän työhön liittyvät hyväksyttyjen luottamuspalvelujen arviointi sekä rajat ylittävään käyttöön ilmoitettujen sähköisen tunnistamisen menetelmien arviointi, jotka voi tehdä akkreditoitu vaatimustenmukaisuuden arviointilaitos. Nykyisin säädetty laissa vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (TunnLL, 617/2009).
  - Jatkossa asetus koskisi myös eurooppalaisia lompakkosovelluksia, joille asetus asettaisi yhteiset vaatimukset. Lompakkosovellusten vaatimustenmukaisuus osoitettaisiin sertifioinneilla. Tarkoitus on, että lompakkosovelluksilta edellytettäisiin myös kyberturvallisuusasetuksen (CSA) mukaista sertifiointia, sitten kun tällainen arviointikriteeristö olisi aikanaan saatavilla. Joka tapauksessa lompakkosovellusten vaatimustenmukaisuutta voisivat arvioida asetuksen (EU) No 765/20081 artiklan 2 kohdassa 13 tarkoitetut vaatimustenmukaisuuden arviointilaitokset.

- Ehdotus COM (2021) 206 final Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen

[1] Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008 , tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta.

unionin säädösten muuttamisesta. Tekoälysäädöksessä ehdotetaan, että suuririskisille tekoälyjärjestelmille olisi tehtävä vaatimustenmukaisuuden arviointi ennen kuin ne saatetaan markkinoille tai otetaan käyttöön. Muiden kuin suuririskisten tekoälyjärjestelmien tarjoajia olisi kannustettava laatimaan käytännesääntöjä, joilla pyritään edistämään suuririskisiin tekoälyjärjestelmiin sovellettavien pakollisten vaatimusten vapaaehtoista soveltamista. Suuririskisten tekoälyjärjestelmien, jotka on sertifioitu tai joista on annettu vaatimustenmukaisuusilmoitus kyberturvallisuusasetuksen (CSA) mukaisessa kyberturvallisuusjärjestelmässä ja joiden viitetiedot on julkaistu Euroopan unionin virallisessa lehdessä, oletetaan täyttävän tekoälysäädöksen 15 artiklassa vahvistetut kyberturvallisuusvaatimukset siltä osin kuin kyberturvallisuussertifikaatti tai vaatimustenmukaisuusilmoitus tai niiden osat kattavat kyseiset vaatimukset.

- Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Tietosuojalain (1050/2018) 14 §:n 4 momentin mukaan Suomessa tietosuojan sertifiointielinten akkreditointitehtävä on annettu tietosuojavaltuutetulle. Tietosuojaan liittyvät säännökset ovat tuoneet uusia velvoitteita ja henkilötietojen suojaamisen tarve on entisestään korostunut suhteessa aikaisempiin vaatimuksiin suojata viranomaisten käsittelemää tietoa.

- Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta (CER). CER-direktiivi tuli voimaan 16.1.2023 ja velvoitteiden kansallinen soveltaminen alkaa 18.10.2024. CER-direktiivin kansallisen toimeenpanon säädösehdotukset ovat valmistelussa.

- Ehdotus COM (2022) 454 final Euroopan parlamentin ja neuvoston asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta (CRA). CRA-ehdotuksen lähtökohta vaatimustenmukaisuuden arvioinnille olisi valmistajan itsearviointi ja tavanomaista korkeamman kyberriskin omaavien tuotteiden osalta ulkopuolisen arviointiorganisaation toimesta osoitettu vaatimustenmukaisuus. Tarkoitus on hyödyntää kyberturvallisuusasetuksen (CSA) mukaista sertifiointia. Radiolaitedirektiiviin RED (2014/53/EU) tarkoittamien EU-markkinoille saatettavien radiolaitteiden tulee olla uusien tietoturvavaatimusten mukaisia 1.8.2025 alkaen. Laitteiden tietoturvallisuuden arviointi siirtynee CRA-ehdotuksen puitteisiin jollakin aikavälillä.

Yhteenvetona tieto- ja kyberturvallisuutta koskevasta EU-sääntelystä voidaan todeta, että viittaukset kyberturvallisuusasetuksen (CSA) mukaiseen sertifiointiin uusissa EU-säädöksissä ovat ilmeisesti lisääntymässä. Tarpeiden tietoturvallisuuden arviointipalveluille odotetaan kasvavan uusien säädösten myötä. NIS2-drektiivin soveltamisalassa on myös osa julkishallinnosta. Keskeiset kansallisen turvallisuuden toimijat on rajattu soveltamisalan ulkopuolelle. Koska NIS2-direktiivi sisältää mahdollisuuden vaatia kyberturvallisuusasetuksen (CSA) mukaisesti sertifioitujen tuotteiden ja palvelujen käyttöä taikka

sertifioinnin hankkimista, niin arviointilakeja ajantasaistettaessa on tarkasteltava, missä määrin EU-sääntely rajoittaa mahdollisuuksia säätää kansallisesta vaatimustenmukaisuuden arvioinnista. Lisäksi arviointilakien ajantasaistamisessa ja arviointien tehostamisessa tulee laajemminkin huomioida tuotesertifiointien hyödyntäminen julkisen hallinnon tietojärjestelmien teknisessä, fyysisessä ja osin hallinnollisessa vaatimustenmukaisuuden arvioinnissa.

Aikaisemmat selvitykset

Arviointilakien mahdollisia uudistamistarpeita on arvioitu useammassa eri yhteydessä:

- Valtiovarainministeriön selvitys digitaalisen turvallisuuden arviointitoiminnan nykytilasta ja kehitystarpeista (VM 2021). Selvityksessä ehdotetaan arviointilakeihin perusteltuja muutoksia ja painotetaan selkeitä vaatimuksia julkisen hallinnon toteuttamille itsearvioinneille ja ulkopuolisille arvioinneille.

- Valtiovarainministeriön selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä (VM 2021). Verrokkivaltioina olivat Tanska, Ruotsi, Viro, Saksa, Alankomaat ja Singapore. Selvityksen perusteella näillä valtioilla, mukaan lukien Suomi, ei ole EU-säädösten lisäksi yhtenäistä lainsäädäntöä tällä alueella, vaan käytännöt vaihtelevat. Selvityksessä ehdotetaan, että arviointeja toteutettaisiin säännöllisesti tietojärjestelmien elinkaaren aikana, arvioinnissa käytettävät kriteerit olisivat linjassa kansainvälisten standardien kanssa ja myös arviointitoiminnassa mukana olevat henkilöt sertifioitaisiin.

- Arviomuistio julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista (VM 2021:54), jossa arviointilakeja tarkastellaan automaattisen päätöksenteon sääntelyn yhteydessä. Työryhmän näkemyksen mukaan arviointilaki tulisi uudistaa kokonaisuudessaan, koska voimassa oleva säädös on sidottu pelkästään tietoturvallisuuden arviointiin.

- Valtioneuvoston periaatepäätöksessä 10.6.2021 tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Titukri). Ehdotetaan tietoturvallisuuden arviointilaitosten määrän lisäämistä tehostamalla arviointilaitosten hyväksymismenettelyä ja valmistelemalla tämän mahdollistavat lakimuutokset.

- Liikenne- ja viestintäviraston (Traficom) valtiovarainministeriölle laatima muistio arviointilaitostoiminnan kehittämisen sääntelystä 18.11.2022. Muistiossa kuvataan perusteltuja muutosehdotuksia arviointilakeihin sekä niitä tarkentaviin ohjeisiin.

- Puolustusministeriön 22.6.2023 asettaman työryhmän (VN/14953/2023) valmisteilla oleva selvitys koskien puolustusvoimien tietojärjestelmien ja salausratkaisujen auditoinnin ja akkreditoinnin toimivaltaa. Selvitystyön tavoitteena on tuottaa puolustushallinnon esiselvitys siitä, miten puolustusvoimille järjestettäisiin itsenäinen auditointi- ja akkreditointioikeus kansallisiin ja kansainvälisiin tietojärjestelmä-, tietoliikenne- ja salausratkaisuihin. Tämän selvityksen ohella

työryhmän valmisteluun vaikuttavia asioita on käsitelty Puolustusvoimien laatimissa Nato-jäsenyyden seurannaisvaikutusten arvioinneissa.

Arvioinneista

Arviointien ajantasaistamiseen ja tehostamiseen liittyvät myös Suomessa käyttöön hyväksytyt arviointiperusteet ja arviointikriteeristöt. Tiedonhallintalautakunta julkaisi 2.6.2022 suosituksen ”Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö (VM 2022:43) sekä päivityksen (VM 2023:46) 12.6.2023 ja Julkriin perustuvan suosituksen tietoturvallisuudesta hankinnoissa (VM 2023:57). Niiden käyttäminen kansallisissa arvioinneissa on alkanut. Katakri on kansallisen turvallisuusviranomaisen (NSA) julkaisema auditointityökalu. Katakria voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. EU-yhteyksissä arviointiperusteet ovat usein kansainvälisiä standardeja tai skeemoja.

Arviointeja toteuttavat myös yksityisellä sektorilla toimivat hyväksytyt arviointilaitokset. Suomen arviointiliiketoimintamarkkinat ovat pienet. Työryhmän työn fokus on julkisen hallinnon tietojärjestelmien arvioinnissa, mutta ottamalla työssä huomioon myös yksityisen sektorin arviointitarpeet voidaan parantaa arviointipalvelujen saatavuutta myös julkiselle hallinnolle.

VN/36127/2023-VM-2

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Hytönen Tomi 912675661	Ikonen Anna-Kaisa 913080200
2024-02-16	2024-02-22