Dnro Traficom/4655/09.02.00/2023
21.4.2023

Neuvontamuistio tunnistuspalveluiden vuoden 2023 määräaikaisarviointeja varten

Yleistä

Vuoden 2023 määräaikaisarvioinnin tilaamisessa/tekemisessä Liikenne- ja viestintävirasto nostaa tämän muistion avulla eri teemoja esille. Teemat ovat edellisissä määräaikaisarvioissa toistuvia puutteita, tai arviointiprosessin parannusehdotuksia. Neuvonnan tarkoituksena on vähentää tarvetta tarkentaville täydennyspyynnöille ja nopeuttaa arvioinnin käsittelyä sekä tunnistuspalvelun tarjoajalla että virastossa.

Säädökset

Tunnistus- ja luottamuspalvelulain (617/2009) 29 §:ssä säädetään vahvan sähköisen tunnistuspalvelun tarjoajan velvollisuudesta teettää määräajoin palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tunnistus- ja luottamuspalvelulaissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset. Auditoinnin tarkoituksena on arvioida sitä, miten tunnistamispalvelu ja yrityksen toiminta vastaa sille asetettuja vaatimuksia.

Tunnistuspalvelun tarkastuskertomus on voimassa tunnistuslain 31 §:n mukaan arvioinnissa käytetyn standardin määrittelemän ajan, kuitenkin enintään 2 vuotta.

Liikenne- ja viestintäviraston oikeudesta antaa tarkempia määräyksiä tunnistuspalvelun vaatimustenmukaisuuden arvioinnissa käytettävistä arviointiperusteista säädetään 42 §:ssä.

Tunnistus- ja luottamuspalvelulaissa sekä siinä viitatuilla osin Euroopan unionin komission täytäntöönpanoasetuksessa (EU) 2015/1502 (varmuustasoasetus) ja sen liitteessä säädetään tunnistuspalvelulle asetetuista edellytyksistä.

Liikenne- ja viestintäviraston määräyksen M72B/2022 15 kohdassa tarkennetaan vaatimusalueet, joiden täytyy sisältyä riippumattomaan arviointiin. Määräyksen 16 kohdassa tarkennetaan vaatimusalueet, joista tunnistuspalvelun tarjoaja voi esittää oman selvityksen.

Liikenne- ja viestintäviraston ohje 211/2019 O 'Sähköisen tunnistuspalvelun arviointiohje' sisältää tunnistuspalvelujen auditoinnin tueksi laaditun yleisen arviointikriteeristön sekä mobiilitunnistusratkaisun erityiskriteeristön. Tunnistuspalvelun tarjoajat voivat käyttää mainittuja kriteeristöjä taikka jotakin toista määräyksen M72B 15 kohdan vaatimukset täyttävää kriteeristöä tai kriteeristöjen yhdistelmää.

Aikataulu

Määräaika toimittaa tarkastuskertomukset liitteineen Liikenne- ja viestintävirastolle on 31.12.2023.

Määräaikaisarvioinnin saa toimittaa virastolle myös aikaisemmin, eikä se vaikuta seuraavan arviointikierroksen aikatauluun.

Muiden arviointien tai sertifiointien käyttäminen

Mikäli vuosina 2022 ja 2023 on suoritettu tunnistusjärjestelmään kohdistuvia arviointeja, voi niitä käyttää osana määräaikaisarviointia eikä arviointia tarvitse tehdä niiltä osin uudestaan, jos arvioitu kokonaisuus ei ole muuttunut arvioinnin jälkeen. Arvioinnit toimitetaan virastolle, vaikka ne olisi jo aiemman muutosilmoituksen yhteydessä toimitettu.

Sertifiointeja voi hyväksilukea siltä osin kuin ne vastaavat tunnistuslain ja määräyksen M72B säännöksiä. Virastolle toimitetaan selvitys siitä, minkä osuuden tunnistuspalvelun arvioinnista sertifiointi kattaa ja miten vastaavuus tunnistuslakiin ja määräykseen M72B/2022 on arvioitu.

Määräaikaisarvioinnissa vuonna 2023 huomioitavat asiat

Auditoijan huomiot ja korjaukset

Jos arvioinnissa huomataan heti korjattavia poikkeamia, ne tulisi huomioida virastolle toimitettavassa materiaalissa. Toimijan tulisi kirjata auditoijan huomiot virastolle toimitettavaan exceliin, sekä vastata huomioihin samassa yhteydessä.

Mikäli tarvittavia korjauksia on mahdollista tehdä, ne tulisi tehdä heti ja huomioida virastolle toimitettavassa materiaalissa. Mikäli arviointiraportissa on havaittu puutteita, eikä korjauksia ole mahdollista tehdä heti, tulisi tunnistuspalvelun tarjoajan toimittaa näihin puutteisiin kattavat selvitykset suunnitelluista korjaavista toimenpiteistä ja niiden aikataulusta.

Tavoitteena on, ettei määräaikaisarviointia koskevaan päätökseen tarvitsisi kirjata asioita, jotka on jo arvioinnissa auditoijan toimesta huomioitu ja merkitty korjattaviksi. Nämä huomiot ovat toimijalla jo tiedossa.

Arvioinnin kesto ja laajuus

Arvioinnin tulee kattaa koko tunnistusjärjestelmä. Arvioinnissa on myös oltava mukana tekniset näytteet (tekninen havainnointi).

Auditoinnin soveltamisalassa on määriteltävä auditoinnin laajuus ja rajat, kuten auditoitavat toimipaikat, organisaatioyksiköt, tietojärjestelmät, toiminnot ja prosessit. Auditoinneissa voidaan käyttää otantaa eli esimerkiksi jokaista toimipistettä ei ole tarve auditoida jokaisella kierroksella. Jos auditointikokonaisuus koostuu useammasta kuin yhdestä auditoinnista on auditointien kokonaisuudessaan kuitenkin kohdistuttava koko tunnistusjärjestelmään.

Päätökseen kirjatut korjausvaatimukset ja korjausten arviointi

Mikäli viraston antamaan päätökseen määräaikaisarvioinnista on kirjattu kriittisiä poikkeamia, jotka vaativat korjausta mahdollisimman pian, tulisi korjaukset toteuttaa ja todentaa tarkastuskäytäntöjen mukaisesti ja toimittaa viraston asettaman määräajan sisällä virastolle valmis vastaus, ei erillisiä liitteitä. Korjauksen todennuksesta olisi hyvä olla mukana arvioijan lausunto.

Tavoitteena on, että pyydetyt korjaukset on joko tehty tai niihin on laadittu korjaussuunnitelma ja tästä toimitetaan virastolle vastaus. Tarkoitus ei ole toimittaa virastolle erillisiä liitteitä siten, että arviointia joudutaan tekemään korjausten läpikäynnin yhteydessä uudelleen viraston toimesta.

Lopettamissuunnitelma

Tunnistuslain mukaisesti tunnistuspalvelun tarjoajalla on oltava kattava suunnitelma tunnistuspalvelun päättämisen varalta. Lopettamissuunnitelman tarkoituksena on olla toimijan apuna mahdollisissa muutos- ja lopetustilanteissa. Olennaista ei ole suunnitelman yksityiskohtaisuus, vaan se, että tarvittavat toimenpiteet ja vaiheet on suunniteltu ja listattu.

Suunnitelmassa tulisi kiinnittää huomiota esimerkiksi järjestelmien mahdolliseen alasajoon, miten ja missä vaiheessa lopettamisesta tiedotetaan käyttäjille, luottamusverkostolle ja luottaville osapuolille ja miten tunnistuslain 24 §:n mukaisesta tietojen säilyttämisestä huolehditaan lopettamisen jälkeen. Lopettamissuunnitelman tulisi olla päivätty ja ajantasainen.

Riskiarvio

Tunnistusmenetelmän on perustuttava riskiarvioon. Tämä tulee liittää osaksi arviointiraporttia. Riskiarvion on osoitettava, että menetelmä ja siihen liittyvät riskienhallintaominaisuudet täyttävät LoA-tason korotettu vaatimukset (esim. kertakäyttösalasanalista, mobiilipäätelaitteen tuettu käyttöjärjestelmäversio jne). Soveltuvuuden voi osoittaa hyökkäyspotentiaalin laskemisella.

Virastolle raportointi ja excel-pohja

Virasto on luonut arviointia varten mallin raportointitaulukosta. Määräaikaisarviointien sujuvuuden kannalta olisi suotavaa, että kyseistä taulukkoa käytettäisiin arviointilaitoksen tuottaman sanallisen arviointiraportin tukena/liitteenä määräaikaisarvointien yhteydessä.

Taulukkoa käyttämällä tunnistuspalvelun tarjoaja voi myös helpommin kilpailuttaa arviointeja ja toisaalta varmistua, että kaikki tarvittavat osat tulee arvioitua. Taulukko perustuu viraston arviointikriteeristöihin viraston ohjeessa 211/2019 O. Sekä taulukko että ohje 211 päivitetään kevään 2023 aikana. Mikäli arvioinnit ovat käynnissä ennen uuden ohjeen julkaisua, toimijan on varmistettava, että määräyksen M72B muutokset tulevat huomioiduksi arvioinnissa.

Virasto muistuttaa vielä, että mitä kattavammat arviointiraportit ja liitteet virastolle toimitetaan, sitä paremmin saadaan määräaikaisarvioinnin tarkastus tehtyä. Myös annetuista määräajoista tulee pitää kiinni, jotta arviointikierrosten aikataulu saadaan vakioitua ja korjauksille annetut määräajat pysyvät tasapuolisina.