TRAFICOM
Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

VÄLIRAPORTTI

Liikenne- ja viestintäministeriö

Päiväys/Datum
27.5.2019
Dnro/Dnr
1448/04/2018
Viite/Referens
Toimenpidepyyntö LVM/2435/02/2018, väliraportti 31.5.2019

Liikenne- ja viestintäviraston väliraportti liittyen liikenne- ja viestintäministeriön toimenpidepyyntöön

1. Selvityspyynnön sisältö

Liikenne- ja viestintäministeriö (LVM) on 19.12.2018 antamassaan toimenpidepyynnössä edellyttänyt Liikenne- ja viestintävirasto Traficomia kohdistamaan liikenteen keskeisiin palveluihin tietoturvallisuuden auditoinnin sekä raportoimaan, miten virastossa on kehitetty tietosuojaan liittyviä prosesseja ja miten virasto järjestää sisäisen tietoturvallisuuden ohjauksen. Auditoinnin tulee valmistua vuoden 2019 loppuun mennessä. Traficomin tulee toimittaa väliraportit 31.5.2019 ja 30.9.2019 mennessä. Loppuraportti tulee toimittaa 16.12.2019 mennessä.

Tässä väliraportissa kerrotaan johtopäätökset joulukuussa 2018 tehdystä tietoturvatarkastuksesta, kevään aikana toteutetuista tietoturvaa ja tietosuojaa parantavista toimenpiteistä, tietoturva-auditoinnin tilanteesta sekä kuvauksia kehittämisen mallista ja viraston tietoturvallisuuden ohjauksesta. Selvityksen edellyttämät toimenpiteet ovat kesken ja jatkotoimenpiteitä tehdään loppuvuoden ajan.

2. Johtopäätökset joulukuussa 2018 suoritetusta tietoturvatarkastusta

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Kuljettajatietojen laaja kyselyiden mahdollisuus ei johtunut tietoturvallisuuden puutteista, vaan itse palveluun tehdyistä asetuksista.

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Kuljettajatiedot-palvelun lisäksi päätettiin joulukuussa 2018 sulkea viisi muuta palvelua tilanteen hallitsemiseksi ja tietosuojan varmistamiseksi.

3. Tehdyt toimenpiteet tietosuojan ja tietoturvan varmistamiseksi

Traficom on arvioinut suljettuina olevat tietopalvelut (julkiset yksittäiskyselypalvelut) ja arvioinut tietopalvelujen tietosuojaa ja henkilötietojen käsittelyn lainmukaisuutta sekä palvelujen tietosisältöä huomioiden kunkin palvelun käyttötarkoituksen, johon palvelu on suunniteltu. Arvioinnissa on kiinnitetty huomioita tietosuoja-asetuksen tietosuojaperiaatteisiin, esimerkiksi henkilötietojen käsittelyn minimointiin.

Arviointityö on dokumentoitu käyttöönottosuunnitelmina sekä jokaisesta palvelusta on laadittu erillinen tietosuojaa koskeva vaikutustenarviointi (DPIA), joka on sisällöltään salassa pidettävää tietoa (STIV, käyttö rajoitettu). Tämä dokumentaatio on läpikäyty yhdessä Liikenne- ja viestintäviraston tietosuoja- ja tietoturva-asiantuntijoiden kanssa ja palveluun on tehty tarvittavat muutokset EU:n tietosuoja-asetuksen säännökset ja muu lainsäädäntö huomioiden.

Traficom on käyttänyt arviointityöhön tasapuolisuuden ja läpinäkyvyyden varmistamiseksi myös ulkopuolisia asiantuntijatahoja. Asianajotoimisto Castrén & Snellman Oy on arvioinut palveluiden laillisuusnäkökulmia. Nixu Certification Oy on auditoinut palveluiden tietoturvallisuutta. Lisäksi palveluja arvioitaessa on tehty yhteistyötä Tietosuojavaltuutetun toimiston kanssa.

Asianajotoimisto Castrén & Snellman Oy on arvioinut palveluiden laillisuusnäkökohtia huomioiden erityisesti yleisen tietosuojalainsäädännön vaikutukset. Palvelut ovat olleet arvioinnin kohteena pääasiassa sellaisena kuin ne ovat edellisen kerran olleet tuotannossa. Castrén & Snellmanin esittämiä huomioita palvelujen tietosisällöstä ja henkilötietojen käsittelyn laillisuusarvioinneista on hyödynnetty palveluiden uudelleen määrittelyssä.

Nixu Certification Oy on aloittanut palveluiden tietoturva-auditoinnin, joka on suunniteltu koostuvat useasta vaiheesta. Auditoinnin vaiheet kestävät koko vuoden. Auditoinnissa vaatimusviitekehyksenä käytetään KATAKRI 2015 -vaatimuksia.

Määritettyihin palveluihin on tehty niiden kehitysvaiheessa sekä nyt tehtyjen kehitystoimien jälkeen Nixu Oy:n toimesta tietoturvatestaus, jolla on arvioitu käyttöliittymätoteutuksen asianmukaista tietoturvaa. Tietoturvatestaus on osa viraston normaalia tuotantoonvientiprosessia.

Palvelualustan tietoturvan tilanne

Omatrafi-palvelualusta on kansalaisille tarkoitettu selainkäyttöinen palveluportaali. Viraston palveluportaalissa on noin 350 sähköistä palvelua, joista viisi on kiinni.

Joulukuussa 2018 suoritettiin palveluiden tietoturva-auditointi. Vuoden 2019 aikana toteutetaan monivaiheinen tietoturva-auditointi, jonka ensimmäinen osa toteutettiin kevään aikana.

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Palveluiden tietosuojan ja laillisuusarvioinnin tilanne

Castrén & Snellman Oy (C&S) on tarkastellut suljettuina olevien palveluiden laillisuusnäkökohdat palveluittain. C&S on arviossaan todennut, ettei voida sanoa palveluissa luovutettavan tietoja selvästi palveluja koskevan lainkohdan sanamuodon salliman ylittävällä tavalla. C&S on kiinnittänyt huomiota muun muassa luovutettavien verotietojen laajuuteen, tietojen hakukriteereihin ja hakutulosten rajoittamiseen, mitkä on huomioitu palveluun tehdyissä muutoksissa.

Liikenne- ja viestintäviraston suorittamissa vaikutustenarvioinneissa on katsottu, että kevään aikana tehtyjen muutosten jälkeen palveluista luovutettavat tiedot ovat liikennepalvelulain mukaisia ja palveluihin tehtävät tekniset rajoitustoimenpiteet varmistavat palvelun käyttöä yksittäisluovutuksiin.

Tietosuojan toteutumisen varmistamiseksi on tehty ja tehdään toimenpiteitä ennen avaamista.

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Palveluiden tietoturvan tilanne

Palveluiden tietoturvan varmistamiseksi on tehty ja tehdään toimenpiteitä ennen avaamista.

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

4. Jatkotoimenpiteet palvelualustan ja palveluiden kehittämiseksi

Omatrafi-palvelualusta

Omatrafi-palvelualustaan tehdään muun muassa seuraavia kehitystoimenpiteitä:

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

- Viraston tulee arvioida yleisesti ICT-sopimusten sisältöä ja käytettävyyttä sekä toimintamalleja ja tehdä tarvittavat korjaukset niihin.

Julkivallu-palvelu

[Poistettu julkisuuslain 24 §:n 1 momentin 7 kohdan nojalla salassa pidettävä tieto]

Suljettuina olevat palvelut

Suljettuina olevien palveluiden (julkiset ajoneuvotiedot ja veron maksu -palvelu, julkiset kuljettajatiedot -palvelu, julkiset ilma-alustiedot -palvelu, julkiset vesikulkuneuvotiedot -palvelu ja merenkulun pätevyystiedot -palvelu) korjaustoimenpiteet ovat käynnissä ja päätös palveluiden avaamisesta tehdään palvelukohtaisesti, kun raportti tehdyistä korjaustoimenpiteistä on saatu ja se on käsitelty viraston riskienhallintaprosessin mukaisesti.

5. Tietosuojaan liittyvien prosessien kehittäminen

Virastossa (Trafi) ei ole aiemmin ollut vakioitua toimintatapaa tietosuojariskien hallitsemiseksi palveluiden koko elinkaaren ajan. Traficomissa on käynnistetty keväällä kehittämisen toimintamalli, joka ottaa kantaa mm. tietosuojaan ja tietoturvaan.

Suljettuina olevien palveluiden käyttöönottosuunnitelmien ja vaikutustenarviointien valmistuttua kehitystyötä on arvioitu ja tarkennettu yhdessä palvelun toteuttavien kehitystiimien kanssa. Käyttöönottosuunnitelmien mukaisten liiketoimintavaatimusten ja tietosuojaperiaatteiden noudattaminen testataan ennen tuotantoon vientiä.

Kuljettajatietopalvelun määrittämiseen ja käyttöönottoon liittyvää päätöksentekomenettelyä arvioitiin vuoden alussa sisäisessä selvityksessä. Puutteita on ollut tietosuojaan liittyvien riskien käsittelyssä ja arvioinnissa. Projektin määrittelyssä tehdyt muutokset taikka testauksissa tehdyt löydökset eivät ole johtaneet riittävään tietosuojan uudelleen arviointiin. Myös projektin dokumentoinnin tarkkuudessa olisi ollut parantamisen varaa.

Kehittämisen toimintamalli

Toimintaa on tehtyjen havaintojen perusteella kehitetty alkuvuodesta 2019 saakka. Kehittämisen toimintamallin mukaisissa projekteissa ja hankkeissa tietosuoja on sisäänrakennettuna malliin. Kehitettävään kohteeseen liittyvät henkilötietojen käsittelytoimet dokumentoidaan koko tiedon elinkaaren ajalta. Projektin tai hankkeen konseptointivaiheessa kehitystiimin avuksi tuotetaan erillisen tiimin toimesta tietosuojan, tietoturvan, riskienhallinnan, tiedonhallinnan ja arkkitehtuurin osalta ylätason vaatimukset, jotka kehitettävässä kohteessa on huomioitava. Vaatimusten määrittelyssä hyödynnetään ns. kynnysanalyysi kriteeristöä, joka pohjautuu EU:n yleisen tietosuoja-asetuksen vaatimuksiin sekä Euroopan tietosuojatyöryhmän (WP 29) ja Euroopan tietosuojaneuvoston tulkintoihin ja lausuntoihin tietosuojalainsäädännöstä. Kynnysanalyysi auttaa määrittämään minkä tasoista dokumentaatiota (PIA, DPIA) kehitettävään kohteeseen liittyvät henkilötietojen käsittelytoimet edellyttävät.

Tavoitetilassa kehittämisen toimintamallissa on mahdollisesti apuna tietosuojatyökalu, jota voidaan hyödyntää dokumentaation tuottamisessa. Vaihtoehtoisesti malliin tullaan luomaan dokumenttipohjat PIAlle ja DPIAlle. Uusi toimintamalli dokumentaatioineen varmistaa muun ohella tietosuoja-asetuksen mukaista osoitusvelvollisuutta tietosuojaperiaatteiden ja -vaatimusten toteutumisesta henkilötietojen käsittelyssä. Toimintamallissa on tietosuojan tarkastuspiste vaatimusten toteuttamisen tarkistamiseksi projektin/hankkeen loppusuoralla ennen lopputuotoksen käyttöönottoa. Tehty PIA/DPIA katselmoidaan tietosuojavastaavan toimesta ja hän antaa asiasta lausunnon. Projektia/hanketta tuetaan tarpeen mukaan tietosuoja-asioissa koko projektin/hankkeen ajan.

Ennen uuden mallin käyttöönottoa huolehditaan väliaikaisilla ratkaisuilla henkilötietojen käsittelyn dokumentoinnista niissä käynnissä olevissa tai alkavissa projekteissa ja hankkeissa, joihin liittyy henkilötietojen käsittelytoimia. Käytännössä tämä tarkoittaa sitä, että projektin/hankkeen on tuotettava tietosuojan ja tiedonhallinnan tarkastuslistan ohella henkilötietojen käsittelystä kirjallinen tietosuojavaltuutetun ohjeistukseen perustuva vaikutustenarviointi. Vaikutustenarvioinnissa kuvataan kehitettävään kohteeseen liittyvää henkilötietojen käsittelyä, arvioidaan käsittelyn

tarpeellisuutta, oikeasuhteisuutta sekä arvioidaan henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarvioinnit on katselmoitu yhdessä kehitettävän kohteen omistavan liiketoiminnan, tietosuojavastaavan, tietoturvavastaavan ja riskienhallintapäällikön kanssa. Lopullisesta vaikutustenarvioinnista lausunnon antaa tietosuojavastaava.

Tietosuojan asiakaslähtöisyys

Rekisteröity ei Traficomin asiakkaana ole vain henkilötietojen käsittelyn kohde, vaan asiakaslähtöisyys tarkoittaa kiinteää yhteistyötä asiakkaan kanssa, ja hänen tarpeisiinsa vastaamista. Tietosuoja-asetuksen yksi keskeinen periaate on läpinäkyvyys. Asiakkaan tulee saada helposti ja ymmärrettävästi tietoa siitä, mitä henkilötietoja, millä tavoin ja miksi hänen henkilötietojaan käsitellään viranomaisessa. Tietosuojaa on pyrittävä toteuttamaan asiakkaan tiedollista itsemääräämisoikeutta kunnioittaen ja tukien.

Edellä todetun takaamiseksi Traficomin ulkoisille internet-sivuille tullaan tuottamaan Tietosuojaportaali, josta asiakkaat saavat helposti ja kattavasti informaatiota Traficomin lakisääteisten tehtävien yhteydessä tapahtuvasta henkilötietojen käsittelystä. Tätä informaatiota tullaan työstämään asiakkaat osallistaen ja tietosuojan palvelumuotoilun asiantuntijaa hyödyntäen.

Tietosuojapolitiikka

Traficomin tietosuojapolitiikka on hyväksytty 19.2.2019. Politiikan mukaisesti tietosuoja on keskeinen osa Traficomin toiminnan ja palvelujen laatua. Ennakoidulla ja suunnitelmallisesti toteutetulla tietosuojalla rakennetaan luottamusta Traficomin kykyyn käsitellä ja hyödyntää henkilötietoja lakisääteisissä tehtävissään. Viraston strategia ja arvot, periaatteet, linjaukset ja ohjeet antavat pohjan laadukkaalle tietosuojalle.

Politiikan mukaan tietosuoja on Traficomissa osa turvallisuuden hallintamallia ja tietosuoja-riskit käsitellään säännöllisesti osana kokonaisturvallisuuden riskienhallintaa. Virasto rekisterinpitäjänä vastaa siitä, että henkilötietoja käsitellään organisaation toiminnassa laillisesti. Viraston johto vastaa tietosuojan toteutumisesta. Toimialat vastaavat siitä, että tietosuoja-vaatimukset huomioidaan liiketoiminnassa. Vaatimuksia noudatetaan myös viraston lukuun suoritettavassa ja viraston rekisteritietoja hyödyntävässä tietojenkäsittelyssä. Jokaisen traficomilaisen vastuulla on käsitellä työtehtävissään henkilötietoja asianmukaisesti. Tietosuojavastaava neuvoo ja ohjaa henkilöstöä kaikissa tietosuojakysymyksissä.

6. Viraston tietoturvallisuuden ohjaus

Viraston kokonaisturvallisuuden hallintamalli on osa viraston johtamisjärjestelmää. Hallintamallin perustana sovelletaan ISO 27001- tietoturvastandardia. Turvallisuuden johtaminen oli yhtenä painopisteenä virastojen yhdistämistä suunniteltaessa. Toteutettu malli yhdistää aiempien virastojen toimintamalleja sekä hyödyntää yleisesti käytössä olevia ja toimiviksi todettuja toimintatapoja.

Viraston kokonaisturvallisuudesta vastaa viraston pääjohtaja, joka johtaa viraston turvallisuutta strategian ja politiikkojen avulla. Viraston johtoryhmä käsittelee viraston kokonaisturvallisuuteen liittyvät vuosisuunnitelmien mukaiset tai merkittäviin tapahtumiin liittyvät raportit, hyväksyy merkittävät turvallisuuden kehityskohteet ja virastoa koskevat politiikat sekä vastaa viraston tietoturvallisuuden seurannasta.

Turvallisuusjohtaja, johtoryhmän jäsenenä, vastaa viraston sisäisen kokonaisturvallisuuden kehittämisestä. Virastoon uutena toimintona on perustettu Turvallisuustoi-

mintoa, joka ohjaa viraston tietosuoja-, tietoturva-, tilaturvallisuus-, henkilöstöturvallisuus-, riskienhallinta- sekä varautumis- ja jatkuvuusasioita. Turvallisuustoiminnon päätehtävänä on kehittää viraston turvallisuuskulttuuria ja varmistaa toiminnan vaatimuksen mukaisuus periaatteilla, ohjeilla, koulutuksilla ja valvonnalla.

Kuluneena keväänä viraston turvallisuuden johtamisessa on keskitytty erityisesti palveluiden riskienhallintaan, yhteisten käytäntöjen luomiseen sekä turvallisuuskulttuurin havainnointiin ja kehittämiseen.

Helsingissä 27.5.2019,

pääjohtaja Kirsi Karlamaa

turvallisuusjohtaja Jari Ylitalo