Liikenne- ja viestintäministeriö

Päiväys/Datum
16.12.2019
Dnro/Dnr
1448/04/2018
Viite/Referens
Toimenpidepyyntö LVM/2435/02/2018, loppuraportti 16.12.2019

Liikenne- ja viestintäviraston loppuraportti liittyen liikenne- ja viestintäministeriön toimenpidepyyntöön

Sisältö

1 Toimenpidepyynnön ja loppuraportin sisällöt

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.

Liikenne- ja viestintäministeriö antoi virastolle myös tehtäväksi tunnistaa ja raportoida loppuraportissa tietoturvallisuuden keskeisiä vähimmäisvaatimuksia ja toimenpiteitä, joita voidaan hyödyntää LVM:n hallinnonalalla ja koko valtionhallinnossa.

Valtionhallinnossa tietoturvan ja -suojan vähimmäisvaatimuksina tulee noudattaa lainsäädännön, asetusten ja vahti-ohjeistuksen sekä muiden riskiperusteisten viitekehysten vaatimuksia.

Tässä raportissa tuodaan esille, miten Traficom on soveltanut näitä edellä mainittuja vaatimuksia käytäntöön vuoden aikana saatujen oppien ja keskeisten havaintojen pohjalta tietoturvan, tietosuojan ja riskienhallinnan parantamiseksi.

Tässä loppuraportissa kerrotaan myös keskeiset muutokset suhteessa edelliseen syyskuussa jätettyyn väliraporttiin sekä keskeisten palvelujen tietoturvallisuuden auditointien ja tarkastusten tämän hetkisestä tilanteesta. Raportissa käsitellään niin ikään myös muita prosessin aikana esiin nousseita yleisempiä huomioita.

2 Suljettujen palveluiden keskeiset muutokset suhteessa edelliseen raporttiin

Traficom avasi asiakkaille 19.11.2019 suljettuna olleen Julkiset kuljettajatiedot -sähköisen asiointipalvelun. Palvelu suunniteltiin ja toteutettiin päivitettyjen tietosuojan vaikutustenarviointien sekä tietoturvatarkastusten toimenpidesuositusten pohjalta. Ennen palvelun käyttöönottoa toteutettiin Nixu Oy:n toimesta sovelluksen tietoturvatarkastus.

Keskeisimmät tietoturvaan liittyvät toteutetut muutokset Julkiset kuljettajatiedot –palveluun ovat palvelun siirto vahvan tunnistautumisen taakse ja hakupalvelun kyselykertojen rajoittaminen. Muutoksia kohdistui myös palvelun lokitukseen, hakulogiikkaan ja palvelun palauttaman tietosisällön minimointiin.

Loppuvuoden 2019 aikana on myös suunniteltu ja toteutettu muutoksia vielä suljettuina oleviin palveluihin: Julkiset vesikulkuneuvotiedot, Ilma-alustiedot sekä Merenkulun pätevyyskirjan tarkistaminen -palveluihin. Hyväksytyn toiminnallisen testauksen jälkeen em. palveluiden tietoturvakontrollien toimivuus tarkastetaan ennen käyttöönottoa. Käyttöönotot on suunniteltu tapahtuvaksi alkukeväästä 2020.

3 Keskeisten palveluiden tietoturvallisuuden auditointien ja tarkastusten tilanne

3.1 Tietoturvatarkastusten ja auditointien kohteet

Liikenne- ja viestintäministeriö edellytti virastoa kohdistamaan keskeisimpiin palveluihin tietoturvallisuusauditointeja. Auditointien viitekehyksenä käytettiin KATAKRI

2015 -viitekehystä ja auditoinnit suoritti tietoturvallisuuden hyväksytty arviointilaitos. Vuoden 2019 aikana auditoinnit kohdistettiin viraston sähköiseen Oma Asiointi -palvelualustaan, sähköiseen tiedonvälitysalustaan sekä suljettuina olleisiin julkisiin palveluihin. Parhaillaan on käynnissä eurooppalaisten viranomaisten tiedonvaihtoon käytettyjen palveluiden viraston rajapintojen auditointi. Osa auditoinneista ja niihin liittyvistä jatkotoimenpiteistä valmistuu vasta vuoden 2020 keväällä.

Lisäksi vuoden 2019 aikana on tehty noin kahteenkymmeneen (20) eri järjestelmään normaaleja viraston toimintatapamallin mukaisia tietoturvatarkastuksia.

KATAKRI 2015 auditointien pohjalta löydettiin palveluista useita kehityskohteita. Kaikkien auditointilöydösten osalta on priorisoitu korkean ja keskitason havaintojen mukaiset korjaus- tai muutostoimenpiteet huomioiden myös kunkin palvelun elinkaari ja toimenpiteiden toteutettavuus. Tietoturvatarkastuksista on saatu useita tärkeitä palvelukohtaisia huomioita kehityskohteista, jotka on voitu ottaa huomioon jatkokehityksessä ja/tai korjata välittömästi.

3.2 Auditointien ja tarkastusten jatkuminen

Eurooppalaisten viranomaisten tiedonvaihtoon käytettyjen palveluiden lisäksi seuraavaksi auditoidaan virastouudistuksen yhteydessä Traficomin vastuulle sovittuja tietojärjestelmiä, jotka ovat siirtyneet sellaisenaan Väylä-virastosta sekä muita keskeisimmiksi arvioituja palveluita ja järjestelmiä. Vuonna 2020 tietoturvan auditoinnit kohdennetaan yhteensä seitsemään priorisoituun järjestelmään.

Näiden lisäksi tehdään edelleen erillisiä tietoturvatarkastuksia kaikkiin tietojärjestelmäkehityksessä oleviin uusiin järjestelmiin sekä tuotannossa olevien järjestelmien keskeisiin muutoksiin. Virastossa hyödynnetään uhka-analyyseja ja –mallinnuksia IT-palvelukehityksen tukena muun muassa arvioimaan erillisten auditointien tai tarkastuksen tarvetta sekä soveltuvinta ajankohtaa.

4 Tietosuojaan kohdistetun sisäisen tarkastuksen tulokset

Tietosuojaa on kehitetty myös toteuttamalla tietosuojan sisäinen tarkastus ulkopuolisen tarkastajan toimenpitein.

Tarkastuksessa esiin nousi kehityskohteina muun muassa ohjeiden velvoittavuuden tulkinnanvaraisuus, kehitystehtävien suuri määrä, projekteihin vaikuttavan toimintaympäristön kartoitus, seuranta ja arviointi palvelun toiminnallisuuksien vaikutuksen arvioinneissa ja se, ettei aikaisemmassa kehittämisen toimintamallissa tietosuojaa ja tietoturvaa ole huomioitu kokonaisuutena.

Näihin suosituksiin liittyen Traficom on suunnitellut ja pääosin jo tehnyt korjaavia toimenpiteitä. Esimerkiksi Traficomin uusittu kehittämisen toimintamalli otettiin käyttöön syyskuun alussa. Menettelyllä varmistetaan mm. kehitystehtävien tietosuojan ja -turvan vaatimuksenmukaisuus sekä kontrollien toteuttaminen kustannus- ja resurssitehokkaasti. Riskienhallinta on jatkuva prosessi kehittämisen elinkaarella ja siinä huomioidaan projektin aikaisten riskien lisäksi etenkin tuotettavan palvelun tai uuden toimintamallin riskit.

5 Oppeja virastossa havaituista henkilötietojen tietoturvaloukkauksista

Liikenne- ja viestintäviraston tietopalveluiden toimintaympäristöön vaikuttavat tietosuoja-asetus ja sen soveltaminen sekä toimintakulttuurin muutokset, minkä johdosta tietopalvelun toimintamalleja on perusteellisesti arvioitu uudelleen erityisesti tietosuojan ja tietoturvan näkökulmasta. Tietopalveluiden toimintojen työohjeita ja

prosesseja on tarkistettu sekä tarvittavin osin täsmennetty ja muutettu. Erityisesti rekisteröidyn oikeuksiin vaikuttavien tietopalveluiden toimintojen prosesseja on päivitetty ja prosessit ovat edelleen kehityksen alla.

Kehitystyössä pyritään tunnistamaan ja ymmärtämään asiakkaiden tarpeet, jotta palvelut olisivat mahdollisimman asiakasystävällisiä, sujuvia ja tietosuojaa toteuttavia. Asiakaskokemusten parantamiseksi tietopalveluihin liittyvää asiakaspalvelua on kehitetty ja yhdenmukaistettu muun ohella asiakasviestinnän ohjeistuksella ja asiakaspalvelun koulutuksella. Tietopalveluiden asiakaspalautteiden käsittelyyn on luotu uusi prosessi käsittelyn säännönmukaistamiseksi ja johdonmukaistamiseksi.

5.1 Yleistä turvallisuuspoikkeamien käsittelystä virastossa

Henkilöstöä on ohjeistettu ilmoittamaan mahdolliset turvallisuuspoikkeamat (ml. tietosuojapoikkeamat) matalan kynnyksen periaatteella; pelkkä epäily mahdollisen poikkeaman olemassaolosta on ilmoitettava asia. Ilmoitukset tehdään esimiehen ohella turvallisuustoiminnolle. Turvallisuustoiminto käsittelee ilmoitukset päivittäin ja varmistaa poikkeamahallintaprosessin käynnistymisen. Poikkeamahallinnalla tarkoitetaan turvallisuuspoikkeaman havaitsemisen jälkeistä prosessia, jossa pyritään;

- estämään poikkeaman laajeneminen
- minimoimaan sen virastolle aiheuttamat vahingot
- käynnistämään toimenpiteet tilanteen korjaamiseksi ja
- palautumaan mahdollisimman nopeasti ja tehokkaasti takaisin normaalitilanteeseen

Turvallisuustoiminto tai tietohallinto yhdessä muiden asiaan liittyvien toimijoiden kanssa luokittelee poikkeaman akuuttien toimenpiteiden jälkeen. Käytössä on viisiportainen asteikko, jossa poikkeama luokitellaan sen vakavuuden mukaan; kriittinen, vakava, merkittävä, lievä ja muu ilmoitus.

Poikkeamille pyritään löytämään ns. juurisyy ja selvittämään poikkeamaan johtanut tapahtumaketju. Tapauksen johdosta järjestetään tarvittaessa läpikäyntitilaisuus, jotta vastaavat poikkeamat vältettäisiin jatkossa. Samalla tarkennetaan ohjeita ja toimintamalleja.

Poikkeamahallinta käsittää paitsi edellä mainitut toimenpiteet, myös tiedottamisen asiasta kulloinkin ajankohtaisille tahoille. Poikkeamahallinnan osalta ulkoisessa ja osin sisäisessäkin tiedottamisessa hyödynnetään viraston kriisiviestintäohjeistusta.

5.2 Henkilötietojen tietoturvaloukkaus turvallisuuspoikkeamana

Virastossa on kuvattu määrämuotoinen prosessi henkilötietojen tietoturvaloukkauksien käsittelemiseksi. Prosessikuvaus on henkilöstön saatavilla viraston intranet sivuilla. Prosessi on myös koulutettu henkilöstölle. Prosessikuvauksen ohella virastossa on tuotettu ns. kysymyspatteristo henkilötietojen tietoturvaloukkauksen kuvaamisen tueksi ja luonnollisen henkilön oikeuksille ja vapauksille mahdollisesti aiheutuvien riskien arvioimiseksi. Kysymyspatteristo auttaa ilmoituksen tekevää tahoa dokumentoimaan tapahtunutta poikkeamaa. Asianmukainen ja kattava dokumentaatio puolestaan auttaa turvallisuustoimintoa henkilötietojen tietoturvaloukkauksen riskinarvioinnissa.

Riskinarvion perusteella ja tietosuoja-asetuksen edellytysten täyttyessä tehdään poikkeamasta ilmoitus tietosuojavaltuutetulle ja mahdollisesti myös loukkauksen

kohteena oleville rekisteröidyille. Tietosuojavastaava esittelee asian viraston turvallisuusjohtajalle, joka hyväksyy ilmoituksen/ilmoitukset. Virastossa tehdään usein ilmoitus loukatulle osana tapahtuman korjaavia toimenpiteitä ilman, että tietosuoja-asetuksen asettamat kriteerit tätä edellyttävät.

Mikäli tehdyn riskiarvion perusteella havaitaan kehittämistoimenpiteitä, turvallisuustoiminto dokumentoi toimenpiteet, vastuuhenkilön ja aikataulun sekä valvoo toimenpiteiden toteutuksen. Turvallisuustoiminto raportoi viraston johdolle säännöllisesti tapahtuneet henkilötietojen tietoturvaloukkaukset.

5.3 Poikkeamista opittua

Virastossa on tunnistettu tarve erityyppisille dokumentaatiopohjille riippuen henkilötietojen tietoturvaloukkauksen luonteesta. Tällä hetkellä käytössä on kaksi erityyppistä riskinarviointipohjaa, joiden tarkoituksena on sekä tehostaa että nopeuttaa riskinarviointiprosessia, mutta myös varmistaa viraston osoitusvelvollisuuden täyttyminen tietosuoja-asetuksessa edellytetyin tavoin.

Virastossa tapahtuneiden henkilötietojen tietoturvaloukkausten avulla on kyetty tunnistamaan niitä henkilötietojen käsittelytoimia, jotka mahdollisesti edellyttävät tehokkaampia hallintakeinoja luonnollisen henkilön oikeuksille ja vapauksille kohdistuvien riskien pienentämiseksi. Nämä kehittämistoimenpiteet on dokumentoitu ja vastuutettu. Lisäksi toimintaprosesseja ja -malleja hallintakeinoineen on kehitetty ja analysoitu yhdessä substanssitoimintojen kanssa tilanteissa, joissa juurisyy poikkeamalle on rekisteröidyn omissa toimenpiteissä, kuten esimerkiksi virheellisen yhteystiedon tai sähköpostiosoitteen ilmoittaminen.

Poikkeamien tunnistamiseen on panostettu sekä koulutuksin että ohjeistusta luomalla ja viestimällä mm. blogikirjoituksin asiasta. Näillä toimenpiteillä virastossa on pyritty luomaan turvallinen ilmapiiri poikkeamista ilmoittamiselle ja saamaan henkilöstö havainnoimaan ja ilmoittamaan aktiivisesti mahdollisista turvallisuuspoikkeamista. Virastossa on tarkoitus tuottaa intranet sivuille anonymisoituja koosteita tapahtuneista poikkeamatilanteista. Poikkeamien ilmoittamisen ohella turvallisuustoiminto kannustaa henkilöstöä tekemään kehitysehdotuksia ja turvallisuusaloitteita.

Rekisterinpitäjän velvoitteiden varmistamiseksi virastossa on aloitettu kaikkien tietopalvelusopimusten läpikäyminen ja uudistaminen. Uusien sopimusten tavoitteena on asettaa tietojen käsittelylle tietosuojan ja tietoturvan kannalta tarkempia ja täsmällisempiä vaatimuksia sekä selkeyttää henkilötietojen käsittelyyn liittyviä vastuita ja rooleja.

6 Havaintojen pohjalta tehtyjä toimenpiteitä tietoturvan, tietosuojan ja riskienhallinnan parantamiseksi

6.1 Palveluiden elinkaari

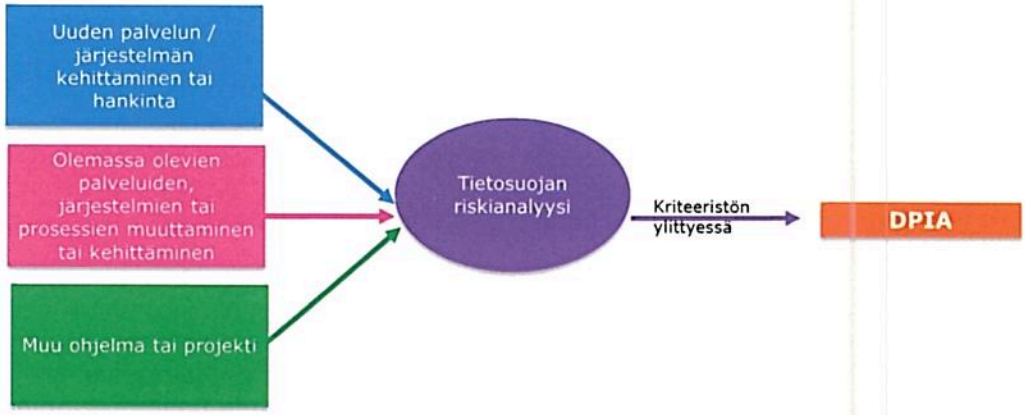
Traficomissa kehitetään palveluiden elinkaaren huomioimista pitämällä yllä tietoja konfiguraatiotietokannassa ja arvioimalla elinkaaren vaatimusten pohjalta tietoturvan ja –suojan riittävää tasoa sekä kehityskohteita.

Palveluiden elinkaaren hallinta alkaa jo kehitysvaiheista, kun palvelua suunnitellaan ja jatkuu läpi palveluhallintaprosessien. Elinkaaren aikana tietosuojan ja –turvan kehitystä seurataan ja kehitetään IT-palvelutuotannossa säännöllisten päivitysten sekä tietojärjestelmien valvonnan, monitoroinnin ja raportoinnin avulla.

Palveluiden elinkaaren arvioinnissa seurataan myös palvelun tuotannon tilaa sekä palvelun ylläpidon kustannuksia. Traficomin virastouudistuksen edetessä arvioidaan myös teknologisia valintoja ja niiden yhtenäistämistä ja em. vaikutusta suhteessa palveluiden elinkaareen.

6.2 Tietosuojariskien arviointi

Traficomissa tietosuojariskejä arvioidaan käyttöön otetun riskianalyysi -työkalun ("kynnysanalyysi") avulla.



Kaavio 1, Tietosuojariskien arviointi

Kynnysanalyysissä kuvataan kohde (mitä ollaan tekemässä ja miksi), kyseessä olevat käsittelytoimet, osapuolet rooleineen sekä vastataan käsittelytoimia, tietosuojaperiaatteita ja rekisteröityjen oikeuksia sekä tietosuojariskien arviointia koskeviin kysymyksiin. Kynnysanalyysi laaditaan moniammatillisissa ryhmissä, joissa huomioidaan tarvittavin osin myös liityntä tietoturvakysymyksiin sekä jäännösriskien arvioimiseen.

Kynnysanalyysi on työkalu ensinnäkin sen arvioimiseksi, onko kyseessä henkilötietojen käsittely. Mikäli on varmistettu, että henkilötietoja ei käsitellä, päätetään kynnysanalyysin laatiminen ja dokumentti tallennetaan.

Kynnysanalyysiä käytetään lisäksi sen arvioimiseksi, onko tarpeen tehdä tietosuojaa koskeva vaikutustenarviointi. Mikäli kynnysanalyysin yhteydessä havaitaan, että korkea riski henkilötietojen käsittelyssä ylittyy, käynnistetään henkilötietojen käsittelyä koskeva tarkempi vaikutustenarviointi -prosessi.

Mikäli kynnysanalyysiä täytettäessä todetaan, ettei vaikutustenarviointia ole tarpeen tehdä, jatketaan kynnysanalyysin laatimista. Valmis kynnysanalyysi katselmoidaan ja jäännösriskit hyväksytetään ennen kohteen käyttöönottoa.

Yllä todetusti vaikutustenarviointi tehdään Traficomissa tilanteissa, joissa kynnysanalyysin perusteella havaitaan, että käsittelytoimiin liittyy korkea riski. Vaikutustenarviointi auttaa ymmärtämään ja käsittelemään henkilötietojen käsittelyyn vaikuttavia tekijöitä, muun ohella henkilötietojen käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä tunnistamaan henkilötietojen käsittelyyn liittyviä riskejä ja riskien vähentämiseen liittyviä toimenpiteitä.

Vaikutustenarviointityötä pidetään Traficomissa osana henkilötietojen käsittelyn suunnittelua sekä olennaisena osana henkilötietojen käsittelyyn liittyvien vaatimusten noudattamista sekä tietosuoja-asetuksen mukaista rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Traficomissa hyödynnetään tietosuojavaltuutetun toimiston ohjeistuksen mukaan laadittua vaikutustenarviointipohjaa. Tietosuojan vaikutustenarviointityötä tehdään moniammatillisissa ryhmissä, joissa, samoin kuin kynnysanalyysiä työstettäessä, huomioidaan tarvittavin osin myös liityntä tietoturvakysymyksiin sekä jäännösriskien arvioimiseen. Valmis riskianalyysi katselmoidaan ja jäännösriskit hyväksytetään ennen kohteen käyttöönottoa.

6.3 Tietosuojaohjeet osaksi palvelukehityksen käsikirjaa

Tietosuojan juridinen viitekehys rakentuu yleisestä tietosuojalainsäädännöstä ja sitä tarkentavasta erityislainsäädännöstä. Viraston turvallisuuden hallintamalli sisältää myös tietosuojan näkökulman. Turvallisuuden hallinnan kannalta keskeinen dokumentaatio on jaettu kolmeen toisiaan täydentävään kategoriaan; politiikat, periaatteet ja suunnitelmat sekä ohjeet. Virastossa on ryhdytty tuottamaan ns. palvelukehityksen käsikirjaa osaksi palveluiden elinkaarta. Palvelukehityksen käsikirja tukee ja on osa turvallisuuden hallintamallia sekä sen dokumentaatiota.

Käsikirja sisältää viraston palveluille asetettavat tietosuojavaatimukset, joita ovat muun muassa tietosuoja-asetuksen tietosuojaperiaatteiden ja sisäänrakennetun ja oletusarvoisen tietosuojan asettamat edellytykset viraston palveluille. Nämä vaatimukset kuvataan sekä 1) tietosuojasääntelystä johdettuina ja "auki kirjoitettuina" vaatimuksina esimerkiksi ohjeistus eri toimijoiden roolien arvioimiseksi henkilötietojen käsittelyssä että 2) konkretian tasolle tuotuina toimenpiteinä palvelujen kehityksessä esimerkiksi viraston sähköisissä asiointipalveluissa edellytettävät toimenpiteet tietosuojavaatimusten täyttämiseksi ja käsittelysäännöt turvakiellon alaisten henkilötietojen käsittelylle.

Palvelukehityksen käsikirja jalkautetaan virastossa sekä koulutuksen että eri verkostojen kautta. Se on myös keskeinen osa viraston kehittämisen toimintamallia ja palveluita kehittävien virastolaisten työkalu tietosuojan sisään rakentamisessa palveluihin.

6.4 Riskienhallinta

Palveluiden suunnitteluvaiheessa on tärkeää hahmottaa ympäristön vaatimukset, reunaehdot, vastuut sekä keskeisimmät riskit, jotta palvelun arkkitehtuuri ja tietoturvakontrollit kyetään suunnittelemaan ja toteuttamaan vaikuttavasti ja mahdollisimman kustannustehokkaasti. Palveluita kehitetään yleisesti erityyppisillä projektimalleilla, joihin riskienhallinta kuuluu kiinteänä osana. Riskienhallintaa tulee arvioida sekä projektin etenemisen, että projektin lopputuloksen näkökulmista. Etenkin jälkimmäinen vaatii arvioijilta paljon, sillä siinä on arvioitava vielä vasta suunnitteilla olevan palvelun eheyttä, käytettävyyttä ja luottamuksellisuutta sekä viraston vastuuta.

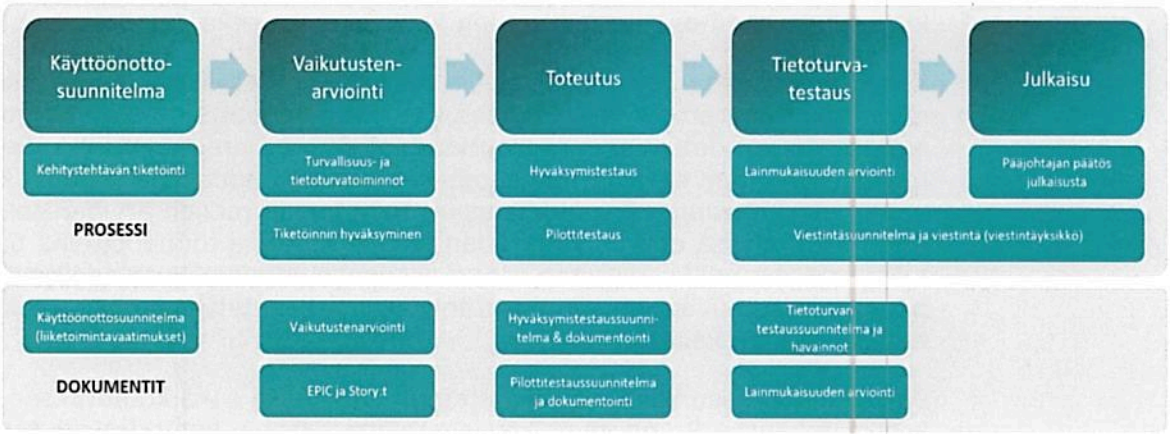
Tuotettava palvelu tulee nähdä osana isompaa kokonaisuutta ja huomioida, ettei asiakas eli kansalainen tai yritys voi valita, kuka tai mikä taho kyseistä viranomaistoimintaa tuottaa. Lisäksi palvelun suunnitteluvaiheessa on kyettävä arvioimaan siihen kohdistuvia väärinkäytön mahdollisuuksia rikollinen näkökulma mukaan lukien. Arvioinnissa on suositeltavaa hyödyntää eri tyyppisiä uhkamallinnuksia.

Virastossa on täsmennetty jäännösriskien käsittelyä ja päätöksentekoa. Riskit tulee käsitellä riittävällä asiantuntijuudella ja tehdä riittävät hallintakeinot riskien pienentämiseksi. Toimintaan jää lähes väistämässä riskejä, joita kutsutaan jäännösris-

keiksi. Virastolla on käytössä hyväksyntätasot, joiden perusteella määrittyy henkilö, joka voi hyväksyä jäännösriskin. Korkeimman jäännösriskin sisältävän päätöksen voi tehdä vain pääjohtaja, alimman tason jäännösriskin voi päättää otettavaksi projektipäällikkö itse. Jäännösriskipäätökset tulee dokumentoida ja mahdollisia jatkotoimenpiteiden toteutumista tulee seurata vastuutaholla.

6.5 Päätökset palvelun käyttöönotossa

Palveluiden uudistamista ja uudelleen käyttöönottoa varten on laadittu tarkennettu toimintamalli, jonka mukaisesti tuotetaan vaadittu dokumentaatio ja toteutetaan palvelun kehitystyö sekä testaus ennen palvelun julkaisupäätöstä. Prosessissa vaaditut asiat toimivat edellytyksenä palvelun käyttöönotolle. Varsinainen käyttöönottopäätös tehdään sen jälkeen, kun erillinen julkaisusuunnitelma todetaan valmiiksi. Palveluiden julkaisun ja käyttöönoton tulee olla johdonmukainen, hallittu ja johdettu prosessi, jonka vuoksi Traficomille rakennettiin erillinen julkaisusuunnitelma.



Kaavio 2, Käyttöönoton prosessi ja dokumentaatio

Julkaisusuunnitelma jakaantuu neljään osaan:

1. ennen julkaisua tehtävät asiat,
2. julkaisun yhteydessä tehtävät asiat,
3. julkaisun jälkeisen asiat ja
4. hätäsulkusuunnitelma.

Suunnitelmassa myös kerrotaan tehtäväkokonaisuudet, tehtävien odotetut lopputulokset ja tehtävien vastuut.

Tietohallinto toteuttaa käyttöönottoja varten oman teknisen käyttöönottosuunnitelmansa, joka synkronoidaan julkaisusuunnitelman kanssa. Tekninen käyttöönottosuunnitelma kuvaa kaikki tarvittavat tietohallinnon ja palvelukumppaneiden tehtävät, jotka valmistelevat, toteuttavat, asentavat, testaavat ja julkaisevat palvelun IT-palvelutuotantoon. Käyttöönottosuunnitelmassa kullekin käyttöönoton tehtävälle on varattu tekijä ja tehtävät on aikataulutettu.

6.6 Kumppanivalvonta ja käytännesäännöt ulkoisille toimijoille

Viraston palveluista osa tuotetaan ulkoistettuna palveluna. Palveluntarjoajat toimivat toimeksiantosopimuksen nojalla tietosuoja-asetuksen mukaisina henkilötietojen käsittelijöinä viraston lukuun. Näitä palveluita ovat esimerkiksi ajoneuvojen ja vesikulkuneuvojen rekisteröinti sekä neuvontapalvelu.

Henkilötietojen käsittelijä saa käsitellä henkilötietoja vain niihin tarkoituksiin ja sillä tavoin kuin virasto rekisterinpitäjänä on määrittänyt. Tietosuojasääntelyssä asetetaan suoraan velvoitteita henkilötietojen käsittelijälle, mutta käsittelystä on lisäksi aina sovittava osapuolten välisellä sopimuksella, jonka vähimmäissisältö on määrätty tietosuoja-asetuksessa. Henkilötietojen käsittelijän täytyy sopimuksen ohella noudattaa rekisterinpitäjän antamia ohjeita henkilötietojen käsittelytoimenpiteille.

Virastossa on aloitettu laatimaan henkilötietoja viraston lukuun käsittelevien palveluntarjoajien käytännesääntöjä. Näiden toimijoita velvoittavien ohjeiden tarkoituksena on yhdenmukaistaa henkilötietojen käsittelyn käytäntöjä toimialalla. Ne toimivat myös osoitusvelvollisuuden työkaluna ja ohjekirjana. Käytännesäännöt tulevat sisältämään yleiskuvauksen viraston toiminnasta ja siihen liittyvästä sääntelykehikosta. Ne täsmentävät ja konkretisoivat henkilötietojen käsittelijöiden velvoitteita.

Tarkoituksena on, että malli hyödynnettävissä myös muualla julkishallinnossa vastaavan tyyppisissä henkilötietojen käsittelytoimissa. Käytännesäännöillä tuetaan tietosuoja-asetuksen asianmukaista soveltamista, sektorin erityispiirteet huomioiden. Hyväksi havaittujen tietosuojakäytäntöjen jakaminen sekä julkishallinnon että yritysten kanssa on muutoinkin virastossa koettu hyödylliseksi ja tarpeelliseksi toimintamalliksi oman toiminnan kehittämisessä. Virasto on käynyt tietosuojakäytänteistä keskusteluja eri toimijoiden kanssa ja hyödyntänyt saatuja oppeja omassa toiminnassa. Yhdenmukaiset toimintamallit julkishallinnossa rakentavat asiakkaiden luottamusta ja yhdenmukaistavat saman tyyppiseen toimintaan liittyvää henkilötietojen käsittelyä.

Ohjeistuksen lisäksi Traficom suorittaa liikenneasioiden rekisterin tietojen käytön valvontaa. Tietojen käytön valvonnan selkeämmäksi kuvaamiseksi virastossa laaditaan uusi valvontasuunnitelma, jonka suunnitteluvaiheessa Traficom on pyrkinyt hakemaan yhtenäiset ja parhaat käytännöt valtionhallinnosta valvonnan suunnitteluun ja toteuttamiseen. Viraston tietojen käytön valvontasuunnitelma on laaja-alainen ja läpileikkaava kuvaus viraston vuosittaisesta tietojen käytön valvonnasta kokonaisuutena. Suunnitelmaan sisältyy valvonnan perusteet, kohteet, tavoitteet, toimenpiteet ja aikataulu valvonnan toteuttamiseksi.

Valvontasuunnitelma on osa tietosuoja-asetukseen sisältyvän rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Valvontasuunnitelman tarkoituksena on varmistaa, että asetuksen tietosuojaperiaatteet toteutuvat kaikessa liikenneasioiden rekisterin henkilötietojen käsittelyssä. Tämä sisältää viraston omassa toiminnassa tapahtuvan henkilötietojen käsittelyn valvonnan, viraston lukuun toimivien palveluntarjoajien henkilötietojen käsittelyn valvonnan sekä niiden palveluntuottajien tietojen käytön valvonnan, joille tietoja luovutetaan liikennepalvelulain VI osan 3. luvussa olevien säädösten mukaisesti.

Valvonnan kautta pyritään ennalta ehkäisemään mahdollisia tietojen väärinkäytöksiä. Lisäksi tavoitteena on varmistaa, että viraston lukuun toimivat palveluntarjoajat ja tietojen luovutuksensaajina toimivat palveluntuottajat käyttävät liikenneasioiden rekisterin tietoja vain sopimuksessa määriteltyyn käyttötarkoitukseen ja noudattavat sopimuksen ehtoja ja vaatimuksia kaikessa henkilötietojen käsittelyssä. Tietojen käytön valvonnan kohteet, toimenpiteet ja havainnot kirjataan erilliseen valvontatyökaluun, joka toimii myös valvonnan raportoinnin välineenä. Tietojen käytön systemaattinen valvonta on aloitettu viraston tietopalveluiden palveluntuottajista ja tietojen käytön valvontaa kehitetään edelleen vuonna 2020. Valvontasuunnitelma laaditaan jokaiselle vuodelle erikseen ja suunnitelmaan kirjataan myös tietojen käytön valvonnan kehittämistoimenpiteet. Kumppanivalvontaa tehdään myös valvomalla ulkoisten kumppanien sopimusten voimassaoloa.

6.7 Tietosuojan johtaminen ja hallinta

Tietosuojan roolit, vastuu ja organisoituminen on määritelty viraston tietosuojapolitiikassa. Politiikan mukaisesti Traficom rekisterinpitäjänä vastaa siitä, että sen henkilötietoja käsitellään organisaation toiminnassa laillisesti. Viraston johto vastaa tietosuojan toteutumisesta. Substanssitoiminnot puolestaan vastaavat siitä, että tietosuojavaatimukset huomioidaan heidän toiminnassaan. 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 ja johtaa tietosuojaverkostoa. Verkoston avulla tietosuojaperiaatteet tuodaan kiinteäksi osaksi operatiivista toimintaa.

Turvallisuustoiminnon tehtävänä tietosuojan osalta on muun muassa linjata, ohjata, valvoa, opastaa ja kouluttaa henkilöstöä tietosuoja-asioissa sekä ylläpitää ja kehittää viraston turvallisuuskulttuuria käyttäen apunaan tietosuojaverkostoa. Viraston tietosuojaverkoston toiminta on käynnistynyt lokakuussa 2019 ja verkostossa on tällä hetkellä 36 jäsentä. Olennaisessa roolissa verkostossa ovat toimialoilta nimetyt henkilöt, joita kutsutaan tietosuojalähettiläiksi. He auttavat omaa toimialaansa tietosuoja-asioissa verkoston tukemana. Verkostossa ei tehdä virastoa koskevia tietosuojapäätöksiä. Nämä päätökset tehdään työjärjestyksen mukaisesti.

Verkoston keskeisenä tehtävänä on edistää informaation jakamista tietosuoja-asioissa läpi koko organisaation ja tukea tietosuojaosaamisen jatkuvuuden hallintaa. Verkostossa kasvatetaan tietoisuutta ja kyvykkyyttä tietosuojaan liittyvien menetelmien käytöstä. Verkosto tuottaa tietoa turvallisuustoiminnolle Traficomin tietosuojan tilasta kokonaisturvallisuuden tilannekuvan täydentämiseksi. Verkostossa käydään läpi tietosuojavaikutuksia sisältäviä ilmiöitä, esimerkiksi poikkeamat, yleisellä tasolla sekä Traficomin tietosuojaan liittyviä linjauksia ja ohjeita sekä tuetaan näiden jalkauttamisessa operatiiviseen toimintaan.

Verkoston toiminnalla tuetaan positiivista ja myönteistä asennetta tietosuojaa kohtaan. Kyse ei ole ylimääräisestä hallinnollisesta taakasta, vaan toiminnan laadun ja korkean tietosuojan tason varmistamisesta. Verkostomainen toiminta tietosuoja-asioissa on virastossa havaittu erinomaiseksi työkaluksi osaamisen jatkuvuuden hallinnassa.

Tietosuojakoulutuksen osalta Traficomissa järjestetään sekä yleistasoista että räätälöityä koulutusta. Traficomin koko henkilöstölle järjestettiin marraskuussa 2019 tietosuojaseminaari. Toimialoilla on myös mahdollisuutta tilata tietosuojalakimiehiltä räätälöityä koulutusta, jonka sisältö suunnitellaan substanssin tarpeiden mukaan.

Tietosuojaa koskevat ohjeet ja työkalut ovat koko henkilöstön saatavilla Traficomin intran tietosuoja -sivuilta, jonne tuotetaan säännöllisesti uutta ohjeistusta havaittujen tarpeiden perusteella. Ohjeissa tietosuojasääntelyn vaatimuksia käännetään käytännönläheisemmälle kielelle ja vaatimuksia avataan myös Traficomin toiminnan kautta esitettävin esimerkein. Tietosuoja -sivuille ollaan tuottamassa myös tietosuojan Q&A dokumenttia, jotta yleisesti esiintyvät sekä substanssikohtaiset tietosuojakysymykset vastauksineen ovat koko henkilöstön saatavilla. Jokainen voi esittää kysymyksiä myös tietosuojalakimiehille, joko suoraan tai ottamalla yhteyttä tietosuojalakimiesten yhteisen yhteydenottokanavan kautta.

6.8 Teknisen tietoturvan toteuttaminen

Tekninen tietoturva on aina mukana IT-palvelujen kehittämisessä ja jatkuvassa IT-palvelutuotannossa. IT-palvelukehityksessä tietoturva lähtee arkkitehtuurisuunnittelusta ja etenee määritysten kautta toteutusvaiheisiin, testaukseen ja lopulta käyttöönottoon. IT-palvelukehitystä tehdään usein ketterin menetelmin ja jaetaan työvaiheita kokonaisuuden kannalta mielekkäisiin osiin.

Teknistä tietoturvaa tukevat viraston määrittämät ei-toiminnalliset vaatimukset, jotka huomioivat tuotettavalle IT-palvelulle edellytettävän tietoturvan vaatimukset. Sovelluskehityksessä hyödynnetään virastossa nk. Sovelluskehityksen pelikirjaa (Software Development Playbook), johon on kuvattu tärkeitä kehityksen ohjeita, linjauksia ja hyödynnettäviä työkaluja. Sovelluskehityksessä on otettu käyttöön useita sisäänrakennettua tietoturvaa varmistavia työvälineitä kohdistuen muun muassa versiohallintaan, yksikkö- ja integraatiotestaukseen, konfiguraationhallintaan ja ohjelmistokoodin laatuun.

Sovelluskehityksessä hyödynnetään tietoturva-asiantuntijoita suunnitteluvaiheissa sekä läpi kehityksen arvioimassa tehtäviä ratkaisuja. Sovelluskehityksessä hyödynnetään myös uhkamallinnusta sekä tietoturvatestausta apuna löytämään tietoturvan kehityskohteita.

Teknisen tietoturvan ylläpito ja jatkuva kehitys vaativat aikaa, työvälineitä ja osaavia resursseja. Virastossa on tarve lisätä tietoturva-asiantuntijoiden määrää, jotta voidaan turvata IT-palvelukehityksen ja tuotannon tuki tietoturvan jatkuvassa kehityksessä.

Toimittajahallinnassa korostuu virastolle IT-palveluja tuottavien toimittajien palvelujen säännöllinen seuranta ja toimittajalta edellytettävä palvelujen vaatimuksen mukaisuuden raportointi, myös erikseen tietoturvasta. Erityisenä havaintona on noussut esiin asiakkaan ja toimittajan välinen tietoliikenteen ohjaus, joka pitää varmistaa. Toimittajalla voi olla kaiken internet-liikenteen ohjaus ulkomaisen palvelun kautta, vaikka varsinaiset palveluohjelmat ja data sijaitsevatkin Suomessa.

Toisena erityishavaintona on kiinnitetty huomiota järjestelmäalustojen päivitysten lisäksi myös muutoksiin palvelimille tehtäviin kovennuksiin. Toimittaja voi sopia valtion edustajan kanssa muutoksista kovennuksiin kertomatta asiaa loppuasiakkaalle. Loppuasiakkaan on oltava tietoinen tehdyistä muutoksista, olivat ne sitten kumpaan suuntaan tahansa.

Virastossa on käynnissä Liikenteen IT-palveluihin liittyvä digiturvallisuuden kehittämishanke, jossa on priorisoitu keskeisimmät tietoturvan kehittämisen tehtävät: tietoliikenteen tietoturva sekä päivitysten ja käyttöoikeuksien hallinta. Lisäksi on käynnissä lokituksen kehittämishanke, jossa tietojärjestelmien toiminnallinen loki ja määritetyt tekniset tiedot ovat hallittavissa keskitetystä järjestelmästä.

Virastossa on kehitteillä myös IT-toiminnanohjausjärjestelmän kehitystyö, joka mahdollistaa jatkossa yhtenäisemmät palveluprosessit, palvelukatalogin, IT assettien (esim. laitteet, ohjelmistot, lisenssit, palvelut) hallinnan ja esim. häiriöiden luokittelun tietoturvapoikkeamiksi tai niiden epäilyiksi yhtenäistä raportointia ja tilastointia varten.

7 Lopuksi

Tietoturvan, tietosuojan ja riskienhallinnan tulee toimia tiiviisti yhdessä toimintoja ja palveluja kehitettäessä. Tätä toimintatapaa on sovellettu Traficomissa kuluneen

vuoden aikana ja se on todettu hyväksi niin toiminnan tehostamisen kuin myös laadun näkökulmasta. Samalla suunnittelua on saatu suoraviivaistettua, muun muassa aiemmin irrallisten tarkastelujen yhteensovittamisten jäätyä pois. Tietosuojan, tietoturvan ja riskienhallinnan tulee olla myös riittävän vahvasti resursoituja.

Kansalaisten tietosuojan ollessa keskiössä, ei mikään toiminnoista sovellu oman toimen ohella hoidettavaksi. Kokemus osoitti, että myös Traficomia edeltäneissä virastoissa ja Traficomin aloittaessa ne ovat olleet vaatimuksiin nähden aliresursoituja. Virasto on ryhtynyt kuluneen vuoden aikana korjaaviin toimenpiteisiin resursoinnin osalta.

Tietoturvaa, tietosuojaa ja riskienhallintaa ei kuitenkaan ratkaista pelkästään tehtävään nimettyjen virkamiesten työpanoksella. Traficom on aloittanut muun muassa koko henkilöstölleen suunnatut tietoturvan/tietosuojan verkkokoulutukset vahvistaakseen ketjun jokaista lenkkiä osana kokonaisvaltaista tietoturvakulttuurin kehittämistä.

Käsiteltäessä julkisia tietopalveluratkaisuja, joissa on tietoja yksittäisten henkilöiden asioista, kuten luvista tai oikeuksista, on hyvä käsitellä asiaa paitsi lainsäädännön, myös käyttäjien (kansalaisten) itsensä kannalta.

Käyttöönotettaessa tai rakennettaessa julkisia palveluita kansalaisten käyttöön tulisi harkita käytettäväksi laajemmin ns. asiakkuusraatia/-paneelia, jonne pyydettäisiin osallistumaan vapaaehtoisia loppukäyttäjiä. Panelisteille kuvattaisiin järjestelmän tai palvelun tavoitetila ja he pääsisivät arvioimaan palvelun tarpeellisuutta, käytettävyyttä ja myöskin tietosuojaa ja tietoturvaa ennen palvelun julkaisua.

Helsingissä 16.12.2019

Pääjohtajan sijainen

Johtaja Jarkko Saarimäki

Turvallisuusjohtaja Jari Ylitalo