

Tietotilinpäätös 2021



Sisällysluettelo

1. Johdon katsaus.....	3
2. Traficomin kokonaisturvallisuuden hallintamalli	5
2.1 Viraston kokonaisturvallisuuden hallinta	6
2.1.1 Henkilöstömme raportoi turvallisuus- poikkeamaepäilyistä	6
2.1.2 Turvallisuuskulttuurin kyselytutkimus	6
2.1.3 Palveluiden tietoturvaluus todennetaan auditoinneilla	7
2.1.4 Turvallisuuden tilannekuva tukee johtamista	7
2.1.5 Turvallisuuden koulutuskatalogi varmistaa osaamisen	9
2.2 Riskienhallinnalla ehkäistään onnettomuuksia ja uhkia	9
2.3 Tietosuojapolitiikka ohjaa henkilötietojen käsittelyssä	10
2.3.1 Tietosuojatiimi ja -verkosto tukevat tietosuojakyvykkyyden kasvua	10
2.3.2 Omavalvonta ja raportointi auttavat tietosuojan toteutumisen varmistamisessa.....	11
2.4 Toimitilaturvallisuus varmistaa häiriöttömän ja turvallisen toiminnan.....	12
2.4.1 Turvallisuusalueet noudattavat vaatimuksia	12
2.4.2 Turvallisuuskontrollit toteutuvat monitasoisesti	12
2.4.3 Turvallisuuskävelyt kehittävät tietoisuutta	12
3. Tiedonhallinta	13
3.1 Tiedonhallintamalli, tiedonohjaussuunnitelma ja asiakirjajulkisuuskuvaus.....	13
3.2 Asian- ja dokumenttienhallinnan tiekartta ohjaa kehitystä ja auttaa viestimään	15
3.3 Lokienhallinnan viitearkkitehtuuri varmistaa yhtenäiset lokihallintakäytännöt	16
3.4 Käyttövaltuuksien hallintaa kehitetään edelleen.....	16
3.5 TIHALA-kehitystehtävä tunnistaa ja vie käytäntöön tiedonhallintalain vaatimuksia.....	16
4. Kokonaisturvallisuuden hallintamalli tukee johtamista	17
5. Kyberturvallisuuskeskuksen vuosi 2021 lukuina.....	19
6. Tietovirtakuvaukset ja toiminnan tunnuslukuja.....	20

1. Johdon katsaus

Tietotilinpäätöksemme täydentää muuta raportointiamme ja sen tarkoituksena on toimia dynaamisena työkaluna, joka tukee organisaation johtamista, raportointia ja kehittämistä. Tietotilinpäätös antaa kokonaiskuvan tietojenkäsittelymme nykytilasta sekä kuvaa tietovarannot ja tietovirrat. Se kuvaa myös tietosuojan ja -turvan sekä tietojenkäsittelyyn liittyvän riskienhallinnan toteutumista toiminnassamme.

Tilannekuva syntyy monesta virrasta

Viime vuonna jatkoimme tietoturvallisuuden ja tietosuojan arviointia säännönmukaisesti eri näkökulmista. Muodostamme turvallisuuden tilannekuvaa muun muassa poikkeamaraporttien, riskiarviointien, palautteen, auditointiraporttien, sidosryhmäyhteistyön sekä omavalvonnan avulla.

Vuonna 2021 kokonaisturvallisuuden hallintamallia arvioitiin ISO 27001 -tietoturvallisuusstandardin näkökulmasta edellisvuosien malliin sisäisillä ja ulkoisilla auditoinneilla vaatimustenmukaisuuden todentamiseksi. Jatkoimme myös palvelujen tietoturvallisuusauditointeja ulkopuolisen tietoturvallisuuden arviointilaitoksen tuella. Poikkeamien seurannasta saamme tietoa kehitystarpeista. Auditointi on meille ennen kaikkea kehittämisen ja jatkuvan parantamisen työkalu.

Prosessien ja riskien hallintaan systemaattisuutta

Kattavalla riskienhallinnalla varmistamme toimintamme jatkuvuuden sekä varautumisen muuttuviin tilanteisiin ja mahdollisiin yllättäviin tapahtumiin. Riskienhallinnan avulla kehitämme resilienssiä.

Tietosuojapolitiikassamme määrittelemme vastuullamme olevien henkilötietojen käsittelyn. Poliitikassa vahvistetaan tietosuoja keskeiseksi osaksi toimintaamme ja palvelujemme laatua. Perustimme jo vuonna 2019 osaksi Turvallisuus-toimintoamme tietosuojatiimin, jonka työtä koordinoi viraston tietosuojavastaava. Lisäksi kehitämme tietosuojan omavalvontaa sisäisillä tietosuojatarkastuksilla.



Vuonna 2021 otimme käyttöön myös uusia toimintamalleja henkilötietojen tietoturvaloukkausten ilmoittamiseksi ja niiden käsittelemiseksi. Teemme tapahtuneesta henkilötietojen tietoturvaloukkauksesta aina dokumentoidun riskiarvion, jonka perusteella voimme tunnistaa toimintaprosesseihimme liittyviä kehittämistoimenpiteitä.

Riskiarvioihin ja tilaluokitukseen perustuvalla toimitilaturvallisuudella turvaamme häiriöttömän ja turvallisen toimitilaympäristön. Tiedonhallintalaki edellyttää meitä varmistamaan, että osana toimitilaturvallisuutta myös tietoaineistot on suojattu fyysisiltä vahingoilta.

Kuvaamme ja ohjaamme tiedonhallintaamme tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksilla, joiden tarkentamista jatkoimme vuoden 2021 aikana. Kehittämisen toimintamallimme painottaa tietosuojan, tietoturvan ja riskienhallinnan merkitystä, ja näin se tukee omalta osaltaan tiedonhallintaamme. Tiedonohjaussuunnitelmassamme kuvataan viraston tehtävät ja niiden käsittelyprosessit, asiakirjatiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat.

Henkilöstöllä turvallisuuden toteutumisessa avainrooli

Koronapandemian aikana olemme kehittäneet toimintatapojamme myös toimivan, turvallisen ja tuloksellisen etätyöskentelyn mahdollistamiseksi. Maaliskuussa 2021 otimme käyttöön koulutuskatalogin, joka sisältää henkilöstöllemme tarjottavat koulutukset muun muassa turvallisuudesta, kehittämisen toimintamallista, riskienhallinnasta, varautumisesta, tietosuojasta ja tietoturvasta.

Meillä Traficomissa turvallisuus on jokaisen asia – otamme turvallisuuden huomioon kaikessa tekemisessämme. Virastomme johto on myös omassa toiminnassaan sitoutunut turvallisuusvaatimusten täyttämiseen ja turvallisuuden jatkuvaan parantamiseen. Tämä on hyvä kasvualusta turvallisuuden hallintamallin kehittämiseen. Konaisturvallisuuden tiedonhallinta ei ole koskaan valmis. Olemme jatkuvan parantamisen polulla.

Kirsi Karlamaa
Pääjohtaja



”Traficomissa turvallisuus on meidän jokaisen asia. Olemme jatkuvan parantamisen polulla.

2. Traficomın kokonaisturvallisuuden hallintamalli

Kokonaisturvallisuuden hallintamallimme pohjautuu ISO 27001 -tietoturvastandardiin ja parhaisiin käytäntöihin. Hallintamalli ottaa kantaa virastomme sisäiseen toimintaan riskienhallinnan, tietoturvallisuuden, henkilöstöturvallisuuden, tietosuojan, tilaturvallisuuden, varautumisen ja jatkuvuuden hallinnan osalta.

Hallintamalli sisältää vastuiden ja roolien määrittelyt, keskeisen dokumentaation, toiminta- ja johtamismallit, henkilöstön tietoisuuden kehittämisen, oikeasuhteiset hallintakeinot, raportoinnin sekä jatkuvan parantamisen mahdollisuuksien tunnistamisen. Malli on johdon hyväksymä. Turvallisuuskulttuurimme rakentuu arvoistamme, arjen käytänteistä ja toiminnasta sekä henkilöstömme asenteista. Turvallisuuskulttuuri ei ole koskaan valmis, vaan se muokkautuu ja sitä muokataan ympäristössä tapahtuvien muutosten johdosta ja virastomme tarpeiden pohjalta.

2.1 Viraston kokonaisturvallisuuden hallinta

2.1.1 Henkilöstömme raportoi turvallisuuspoikkeamaepäilyistä

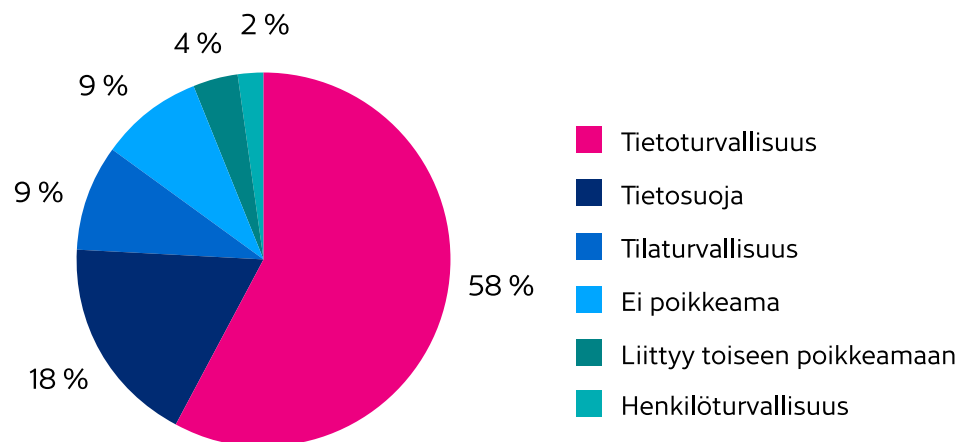
Turvallisuuskulttuurimme yhtenä kulmakivenä on matala kynnyksellä ilmoittaa poikkeamaepäilyistä turvallisuuspoikkeamina. Jokainen poikkeama-ilmoitus käsitellään ja samalla yritetään löytää poikkeaman juurisyy. Toimintamalli tuo esille toimintaamme kohdistuvat uhkat ja realisoituneet riskit. Näin kykenemme jatkossa suojaamaan aiempaa paremmin. Valtaosa henkilöstömme tekemistä poikkeamailmoituksista liittyy

tietojenkalasteluyrityksiin sähköpostitse tai puhelimella. Henkilöstömme kyky tunnistaa tietojenkalasteluyrityksiä kehittyy koko ajan ja aiheesta muistutetaan esimerkiksi koulutuksissa ja intranet-uutisilla. Palautteen perusteella poikkeamista raportoinnin kulttuuri koetaan positiiviseksi ja poikkeamista raportoidaan silloinkin, kun se on johtunut henkilön omasta toiminnasta.

2.1.2 Turvallisuuskulttuurin kyselytutkimuksesta

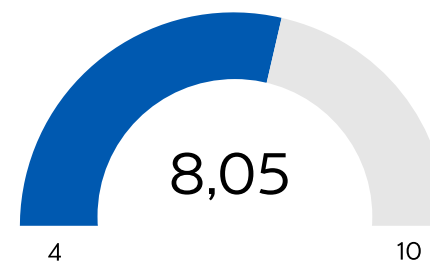
Toteutimme toistamiseen turvallisuuskulttuuriamme mittaavan kyselytutkimuksen henkilöstölle. Vastausprosentti oli 27 (aiemmin 34). Turvallisuuskulttuurillemme annettujen kouluarvosanojen (4-10) keskiarvo pysyi noin kahdeksassa. Oman turvallisuustietoisuuden arvosanojen keskiarvo oli 8,2 (aiemmin 8,3).

Poikkeamailmoitukset

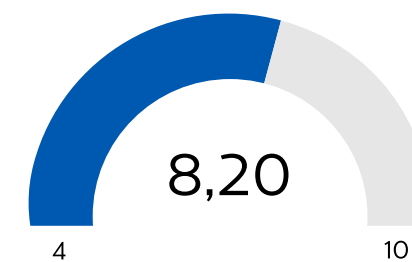


Turvallisuuskulttuuri

Minkä kouluarvosanan antaisit viraston turvallisuuskulttuurille?



Minkä kouluarvosanan antaisit turvallisuustietoisuudellesi?



Riskiarviointeihin osallistuneiden osuus nousi hieman ja oli nyt 53 prosenttia. Laki julkisen hallinnon tiedonhallinnasta (906/2019) muutti salassa pidettävien asiakirjojen luokittelua, minkä johdosta asiasta järjestettiin koulutusta. Annetulla koulutuksella voidaan arvioida olleen merkitystä, sillä tietojen luokitteluosaamisessa oli havaittavissa merkittävää positiivista kehittymistä.

2.1.3 Palveluiden tietoturvallisuus todennetaan auditoinneilla

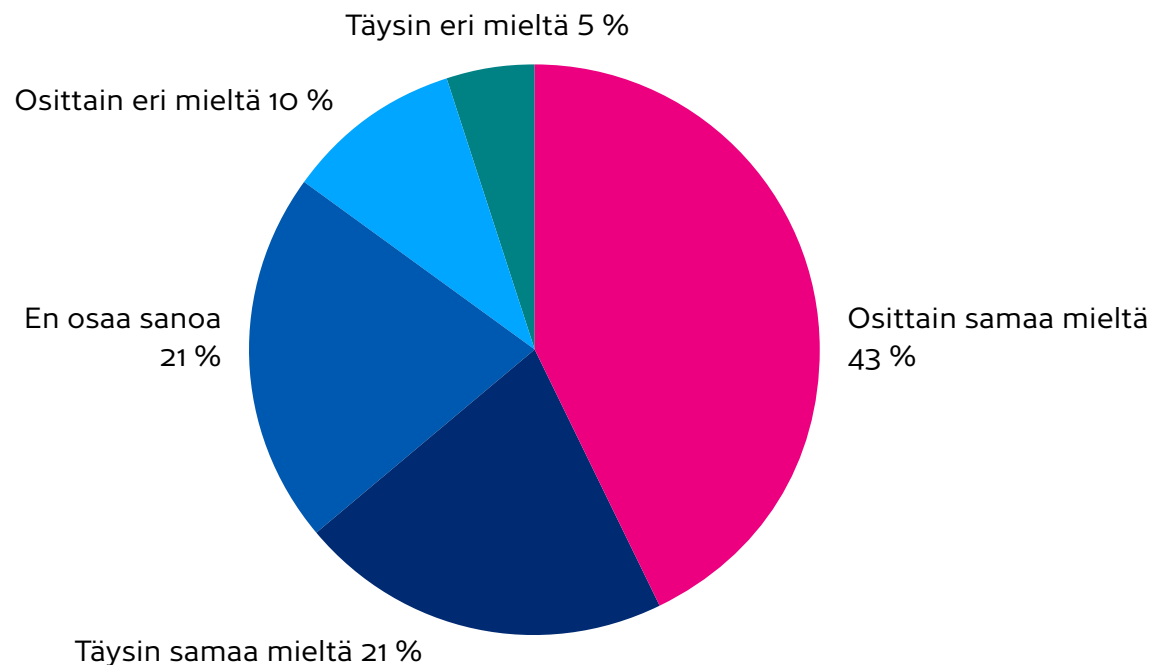
Vuoden 2021 aikana kansallinen turvallisuusauditointikriteeristö eli Katakri 2015 -auditointi kohdistettiin muun muassa viraston uuteen asiointialustaan, jota kansalaiset ja yritykset käyttävät verkkosivujemme kautta. Auditoinnin tavoitteena oli todentaa, että järjestelmä täyttää turvallisuusluokan IV asiakirjojen käsittelyyn tarkoitetun tietojärjestelmän vaatimukset. Katakri-viitekehys oli huomioitu tietojärjestelmän suunnittelu- ja toteutusvaiheessa, joten auditoinnissa ei havaittu yhtään vakavaa poikkeamaa. Auditoinnin lopputulos oli hyvä osoitus siitä, kuinka lopputuloksen ja sujuvan käyttöönoton kannalta on tärkeää huomioida tietoturvallisuusvaatimukset jo järjestelmäkehityksen alkuaskelista alkaen.

2.1.4 Turvallisuuden tilannekuva tukee johtamista

Turvallisuusjohtajamme pitää virastomme johtoryhmän tietoisena toimintaamme vaikuttavista ajankohtaisista turvallisuusasioista ja tulevaisuuden kehityssuunnista. Turvallisuustoiminnon vastuulla on kerätä ja koota viraston turvallisuuden ja riskienhallinnan tilannekuva. Tilannekuva muodostetaan muun muassa poikkeamaraporttien, riskiarviointien, palautteen, auditointiraport-

tien, sidosryhmäyhteistyön sekä omavalvonnan avulla. Raportointi tehdään vuosikellon mukaisesti vähintään kolme kertaa vuodessa. Ensimmäisen vuositertiaalain aikana laadittava raportti on laajin kokonaisuus, joka noudattaa ISO 27001 -standardissa määritettyä johdon katselmuksen sisältöä. Katselmuksen yhteydessä myös varmistetaan, että turvallisuuden hallinnan kannalta keskeinen dokumentaatio vastaa ympäristön ja toiminnan vaatimuksia.

Virastomme turvallisuusjohtaminen tuottaa tulosta



Kokonaisturvallisuuden tilannekuvaprosessi

1. Tiedonkeruu

Toimintaympäristöön ja toimintaan liittyviä tietoja kerätään eri lähteistä ja mittareista ja täytetään keruukortti.

2. Analysointi

Keruukorttien pohjalta muodostetaan ymmärrys tilanteesta ja arvio tulevaisuudesta. Tilannekuva tuote valmistuu.

3. Arviointi

Tilannekuvaa arvioidaan ja täydennetään julkaistavaan muotoon.

4. Esittäminen

Tilannekuva esitetään johtoryhmälle osana johtamisjärjestelmän raportointia.

5. Oppiminen

Tilannekuvaa kehitetään saadun palautteen perusteella, jotta se palvelisi entistä paremmin ylimmän johdon tarpeita.



2.1.5 Turvallisuuden koulutus-katalogi varmistaa osaamisen

Turvallisuuden tuottama koulutuskatalogi, joka sisältää kokonaiskuvan tarjolla olevista koulutuksista henkilöstöllemme, on otettu käyttöön maaliskuussa 2021. Katalogi koostuu muun muassa turvallisuus-koulutuksista, kehittämisen toimintamallin koulutuksista, riskienhallintaan ja varautumiseen liittyvistä koulutuksista, tietosuojakoulutuksista sekä tietoturvaan liittyvistä koulutuksista. Katalogiin on kirjattu koulutuskohtaisesti muun muassa koulutuksen kohderyhmä sekä lyhyt kuvaus koulutuksesta, sen tavoitteista ja kestosta sekä vastuukouluuttajasta. Koulutukset ovat joko etukäteen nauhoitettuja verkkokoulutuksia tai erikseen tilattavia osin räätälöitävissä olevia etäyhteys- ja/tai lähikoulutuksia. Koulutustarjonta kattaa myös perehdytys-koulutuksen uusille traficomilaisille. Koulutus-katalogia päivitetään aina tarpeen mukaan.

2.2 Riskienhallinnalla ehkäistään onnettomuuksia ja uhkia

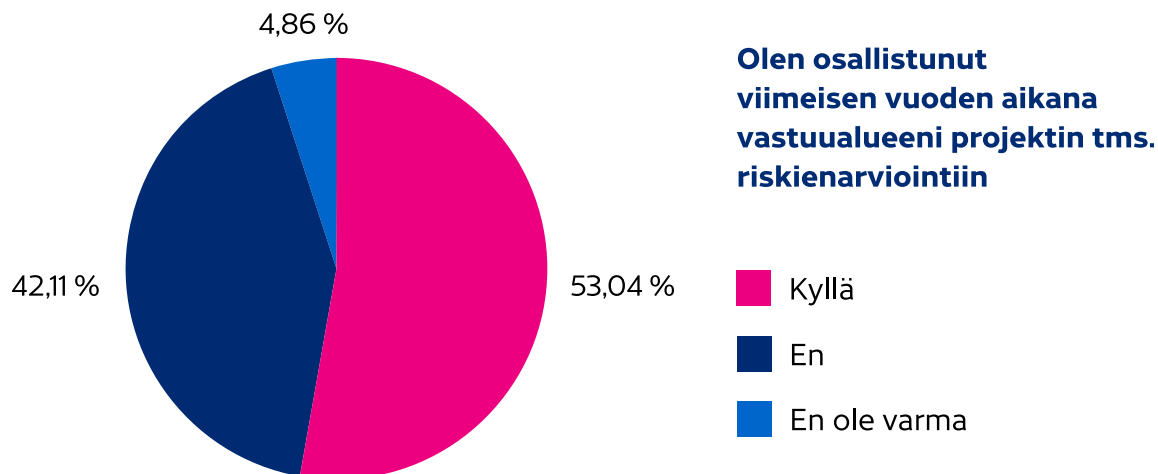
Kokonaisvaltainen, kehittyvä riskienhallinta tukee kokonaisturvallisuuden hallintamallimme toteuttamista. Onnettomuuksien ja uhkien ennakointi ja ennaltaehkäisy ovat riskienhallinnan ydintä. Riskienhallinnalla vähennämme mahdollisten uhkien vaikutuksia virastossamme. Toteutamme riskienhallintaa sisäisesti ja ulkoisesti. Ulkoinen riskienhallinta kattaa toiminnot, joista vastaamme lainsäädännön, sopimusten tai muiden velvoitteiden nojalla. Päivittäisellä, kattavalla riskienhallinnalla varmistamme toimintamme jatkuvuuden sekä varautumisen muuttuviin tilanteisiin ja yllättäviin tapahtumiin.

Päivitämme säännöllisesti johdon vahvistamaan riskienhallintapolitiikkaamme. Se sisältää riskienhallinnan periaatteet, tavoitteet, roolit ja vastuut. Linjausten toteutumisesta vastaa johto.

Osaamisalueet ja toiminnot vastaavat siitä, että riskienhallinta huomioidaan operatiivisessa toiminnassa. Jokaisen traficomilaisen vastuulla on tunnistaa riskit sekä pyrkiä ennaltaehkäisemään niistä aiheutuvia haittoja ja vahinkoja. Meidän jokaisen vastuulla on myös ilmoittaa mahdollisista uhkista, turvallisuuspoikkeamista ja läheltä piti tilanteista turvallisuustoiminnollemme.

Käynnistimme marraskuussa 2019 riskienhallintaverkoston.

Riskienhallintaverkostossamme on tällä hetkellä lähes 20 jäsentä ja kokoontumisia oli yksitoista vuonna 2021. Verkoston keskeisenä tehtävänä edistää tiedon jakamista ja kulkua riskienhallintaan liittyvistä asioista koko organisaatiossa. Haluamme kasvattaa riskienhallintatietoisuutta ja -osaamista. Verkostollamme on tärkeä rooli kokonaisturvallisuuden tilannekuvan täydentämisessä. Verkoston tilaisuuksissa tuodaan esille ajankohtaisia turvallisuuteen vaikuttavia ilmiöitä ja kannustetaan avoimeen keskusteluun. Tapamisissa käydään tarvittaessa läpi turvallisuuden tai riskienhallinnan linjauksia ja ohjeita asian ymmärtämisen ja sitoutumisen varmistamiseksi. Näin edistämme riskienhallinnan periaatteiden tuomista kiinteäksi osaksi arjen toimintaa.





Turvallisuuden osana toimii riskienhallintatiimi, joka tukee ja auttaa traficomilaisia riskienhallinnan kysymyksissä sekä laatii riskienhallintaohjeita käytännön riskienhallinnan tueksi. Tiimi ohjaa, linjaa, opastaa, kouluttaa ja valvoo henkilöstöämme riskienhallinnan asioissa sekä ylläpitää ja kehittää turvallisuuskulttuuriamme.

Riskienhallintakoulutukset ovat riskienhallintatiimin vastuulla. Intranetissämme on koulutus- ja perehdytysvideoita, jotka mahdollistavat kouluttautumisen itselle sopivana ajankohtana. Lisäksi intranetissä on työkaluja ja riskienhallinnan ohjeita. Räätelöityjä koulutuksia tuotetaan tarpeen mukaan.

”Tietosuoja on keskeinen osa toimintaamme ja palvelujemme laatua.

2.3 Tietosuojapolitiikka ohjaa henkilötietojen käsittelyssä

Kokonaisturvallisuuden hallintamallin kannalta keskeiseen dokumentaatioon kuuluvat turvallisuuden osa-alueita koskevat politiikat, jotka täydentävät viraston strategiaa ja työjärjestystä. Tietosuojapolitiikassa määritellään ja ohjataan vastuullamme olevien henkilötietojen käsittelyä. Poliitikassa vahvistetaan tietosuoja keskeiseksi osaksi toimintamme ja palvelujemme laatua. Tietosuoja osana kokonaisturvallisuutta ohjaa ja kehittää virastomme tietosuojakulttuuria.

2.3.1 Tietosuojatiimi ja -verkosto tukevat tietosuojakypsytyksen kasvua

Perustimme vuonna 2019 osaksi Turvallisuustoimintoa tietosuojatiimin, jonka työtä koordinoi viraston tietosuojavastaava. Tiimissä työskentelee kolme tietosuojajuristia ja tietosuojavastaava. Tiimin perustehtävänä on linjata, ohjata, valvoa, opastaa ja kouluttaa henkilöstöä tietosuoja-asioissa sekä ylläpitää ja kehittää viraston turvallisuuskulttuuria tietosuojaverkoston kanssa. Henkilöstömme voi lähettää tiimille tietosuojaan liittyviä tukipyynnöitä keskitetyn yhteydenottokanavan kautta. Tiimi edistää tietosuojaan liittyvää osaamista annettujen linjausten, ohjeistusten ja koulutusten avulla ja pyrkii näin kasvattamaan tietosuojakypsytyttämme.

Tietosuojaverkostonkin toiminta käynnistyi lokakuussa 2019. Verkoston 46 vapaaehtoisesti mukaan ilmoittautunutta jäsentä kokoontuvat pääsääntöisesti kerran kuukaudessa. Aiempien vuosien tapaan verkostossa käsiteltiin vuonna 2021 muun muassa kansallisen tietosuojaviranomaisen antamia linjauksia ja päätöksiä, tietosuoja-asioiden kansallista ja kansainvälistä oikeuskäytäntöä sekä Euroopan tietosuojaneuvoston antamia ohjeita ja suosituksia. Edellä mainittujen kannanottojen vaikutuksia arvioidaan suhteessa omaan toimintaamme.

Tietosuojaverkoston toiminta keskittyi vuonna 2021 aiempaa enemmän ohjeiden viemiseen osaksi päivittäistä toimintaamme sekä vuorovaikutuksen ja tiedonvaihdon vahvistamiseen. Verkosto koulutti traficomilaisia viime vuonna virastossa laadittuja tietosuojaohjeiden osalta, esimerkkinä henkilötietojen käsittelyviranomaisen toteuttamissa kyselytutkimuksissa ja selvityksissä sekä henkilötietojen siirtäminen kolmansiin maihin. Lisäksi verkostossa on pidetty alustuksia sähköisen viestinnän tietosuojasta ja hankintaprosessistamme sekä siinä yhteydessä huomioitavista tietosuoja-asioista, esimerkkinä henkilötietojen käsittelyä koskevat sopimusehdot. Verkostossa etsitään myös yhdessä ratkaisuja mahdollisiin tietosuojaasteisiin. Tietosuojatiimi saa verkostosta hyödyllistä tietoa tarvittavista koulutuksista sekä henkilötietojen käsittelytoimista, joihin tarvitaan virastotason linjausta tai tarkempaa ohjeistusta.

2.3.2 Omavalvonta ja raportointi auttavat tietosuojan toteutumisen varmistamisessa

Virastossamme on määrämuotoinen prosessi henkilötietojen tietoturvaloukkauksien käsittelyyn. Henkilötietojen tietoturvaloukkaus on yksi turvallisuuspoikkeamalaji. Kaikki turvallisuuspoikkeamat saapuvat keskitetysti järjestelmäämme, joka mahdollistaa kattavan seurannan ja tehostaa poikkeamien käsittelyä sekä dokumentointia. Samaa ilmoittamiskanavaa käytetään myös turvallisuusaloitteiden ilmoittamiseen. Intranetissämme julkaistu ohjeistus turvallisuuspoikkeaman ilmoittamiseen sisältää tiedon turvallisuuspoikkeaman käsittelystä, poikkeamahallintaprosessista ja poikkeamien luokittelusta mahdollisten akuuttien toimenpiteiden jälkeen.

Tapahtuneesta henkilötietojen tietoturvaloukkauksesta tehdään aina dokumentoitu riskiarvio, jonka perusteella tunnistamme toimintaprosesseihimme liittyviä kehittämistoimenpiteitä. Suunnitelmat dokumentoidaan, vastuutetaan ja aikataulutetaan, minkä jälkeen toteutumista seurataan ja valvotaan. Toimintaprosessin muutoksista viestitään ja niistä annetaan koulutusta esimerkiksi tietosuojaverkostossamme. Johdolle raportoidaan virastossa tapahtuneet henkilötietojen tietoturvaloukkaukset.

2.4 Toimitilaturvallisuus varmistaa häiriöttömän ja turvallisen toiminnan

Riskiarvioihin ja tilaluokitukseen perustuvalla toimitilaturvallisuudella turvataan häiriötön ja turvallinen toimitilaympäristö, joka hyödyntää vaatimustenmukaista teknistä turvallisuusvalvontaa. Tiedonhallintalaki edellyttää virastoa varmistamaan, että tietoaineistot on suojattu fyysisiltä vahingoilta, kuten tuhoutumiselta ja anastukselta.

2.4.1 Turvallisuusalueet noudattavat vaatimuksia

Toimitilamme on jaettu turvallisuusalueisiin, joihin kohdistuu erilaisia vaatimuksia lainsäädännöstä, standardeista tai viraston ja valtionhallinnon sopimuksista tai ohjeista. Vaatimusten toteuttamiseksi alueille on luotu asianmukaisen turvallisuustason saavuttamiseksi erityyppisiä turvallisuuskontrolleja, esimerkkinä lukitus, kulunvalvonta, kameravalvonta tai rikosilmoitinlaite. Turvallisuusluokiteltujen tietojen (esimerkiksi TL IV – TL I tai vastaavat kansainväliset luokitukset) jatkuva, säännöllinen tai toistuva käsittely ja säilytys vaativat luokituksen mukaista turvallisuusaluetta, kuten hallinnollinen alue tai turva-alue. Tilapäisesti voi olla sallittua käsitellä tietoa myös alemman tason turvallisuusalueella. Tietoturvaohjeemme antavat ohjeistukset vaadittavista tietojenkäsittely-ympäristöistä.

2.4.2 Turvallisuuskontrollit toteutuvat monitasoisesti

Tilojemme turvallisuuskontrollit on toteutettu monitasoisesti. Fyysisten rakenteiden lisäksi näkyvin kontrolli on kulunvalvontajärjestelmä, jolla ohjataan kulkemista, tunnistetaan tiloissa liikkuvat henkilöt ja estetään luvottomien henkilöiden pääsy tiloihin. Kulkuoikeudet määrytyvät henkilön työtehtävien mukaan. Vierailijakäytännöistä on ohjeet, jotka edellyttävät muun muassa vierailijakortin käyttämistä ja saatettuna liikkumista viraston ei julkisissa -tiloissa.

”Arjen toiminta on tärkeää. Lisäämme tietoisuutta esimerkiksi turvallisuus-kävelyillä.

2.4.3 Turvallisuuskävelyt kehittävät tietoisuutta

Kiinnitämme erityistä huomiota arjen toimintaamme. Turvallisuuskontrollimme eivät toimi tehokkaasti, jos henkilöstömme ei ymmärrä niiden merkitystä ja tahattomasti tai tahallisesti heikentää niiden tehoa. Jokainen viraston turva-alueille kulkuoikeudet saava työntekijämme suorittaa turvallisuuskävelyn kulkuoikeuden myöntämisen edellytyksenä. Turvallisuuskävelyn aikana kouluttajamme tutustuttaa henkilöstön paloturvallisuuteen ja pelastautumiseen liittyvien seikkojen lisäksi arjen tietoturvaluuteen. Turvallisuuskävely on kokemuksellinen oppimistapa, joka pidentää muistijälkeä opetetuista asioista.

3. Tiedonhallinta

3.1 Tiedonhallintamalli, tiedonohjaussuunnitelma ja asiakirjajulkisuuskuvaus

Tiedonhallintalaki luo perustan menettelytavoille, joilla viranomainen käsittelee toiminnassaan syntyviä tietoja niiden elinkaaren ajan. Traficomissa tiedonhallintaa kuvataan ja ohjataan tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksella.

Tiedonhallintamallissamme kuvataan tiedonhallintayksikön eli viraston toiminta, tietopääoma ja tietojärjestelmät. Mallissa kuvataan myös toimenpiteet, joilla toteutamme tietoturvasuutta sekä menettelyt tietojenkäsittelyyn, tietojärjestelmien ja tietoaineistojen turvaamiseksi sekä näiden vastuutahot. Olemme jatkaneet vuoden 2021 kuvauksien täydentämistä ja tarkentamista, samalla olemme määritelleet myös tiedonomaistajien vastuut tiedon elinkaaren aikana. Kehittämisen toimintamallissamme painotetaan tietosuojan, tietoturvan ja riskienhallinnan merkitystä kehittämisessä. Malli toteuttaa ja tukee omalta osaltaan tiedonhallintaamme. Se myös mahdollistaa ajantasaisen tiedon keräämisen ja hyödyntämisen tiedonhallinnan muutosvaikutusten arviointia varten.

Tiedonohjaussuunnitelmassamme kuvaamme viraston tehtävät ja käsittelyprosessit, tehtävien hoidossa syntyvän asiakirjallisen tiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat. Yhteensä tehtävä- ja asiaryhmiä on noin tuhat. Tiedonohjaussuunnitelman ylläpito on jatkuva prosessi, jota päivitetään tehtävien muuttuessa. Tiedonohjaussuunnitelma hyväksytään vuosittain ja se on osa tiedonhallintamallia.

Asiakirjajulkisuuskuvaukseemme antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoja lakisääteisissä tehtävissämme. Asiakirjajulkisuuskuvaus toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön sisältö lain viranomaisten toiminnan julkisuudesta (621/1999) 13 §:n edellyttämällä tavalla sekä opastaa tietoaineistojen omatoimisessa haussa ja käytössä. Asiakirjajulkisuuskuvaus on saatavilla [traficom.fi-verkkosivuilla](https://traficom.fi/verkkosivuilla). Päivitämme kuvausta säännöllisesti tietovarantoihin ja tietojärjestelmiin tehtävien muutosten yhteydessä.



Tiedonhallintamallin kokonaisuus



3.2 Asian- ja dokumenttienhallinnan tiekartta ohjaa kehitystä ja auttaa viestimään

Asianhallintajärjestelmissämme käsiteltiin vuonna 2021 noin 631 000 asiaa ja noin 1 123 000 asiakirjaa. Sähköisen asioinnin kasvun ja digitalisaation myötä automaattisesti vireille tulevien asioiden määrä on jatkuvassa kasvussa. Digitoimme vuonna 2021 yhteensä noin kaksi miljoonaa asiakirjaa sähköiseen muotoon.

Laadimme vuonna 2021 asian- ja dokumenttienhallinnan tiekartan, jossa on kuvattu viraston asian- ja dokumenttienhallinnan nykytila ja tavoitetila. Tiekartan tavoitteena on ohjata asian- ja dokumenttienhallinnan suunnittelua sekä toimia kehittämisen tukena ja viestinnän välineenä. Tiekartalle on vaiheistettu asian- ja dokumenttienhallinnan kehittämissuunnitelmamme tuleville vuosille. Vuoden 2021 aikana valmistelimme uutta dokumenttienhallintajärjestelmäämme, joka yhtenäistää ja keskittää dokumenttienhallintamme. Järjestelmä otetaan käyttöön keväällä 2022. Tämän jälkeen ryhdytään suunnittelemaan ja toteuttamaan tiekartan seuraavaa vaihetta eli asianhallinnan kehittämistä ja yhtenäistämistä.

Asian- ja dokumentinhallinta vuonna 2021

Asianhallintajärjestelmissä
käsitellyt asiat
631 000

Digitaalisia asianhallinnan
asiakirjoja
n. 1 123 000

Dokumenttienhallinnan
uusia työtiloja
1 014

Dokumenttienhallintaan
tallennettuja dokumentteja
155 000

”Sähköisen asioinnin kasvun ja digitalisaation myötä automaattisesti vireille tulevien asioiden määrä kasvaa voimakkaasti.

3.3 Lokienhallinnan viitearkkitehtuuri varmistaa yhtenäiset lokienhallintakäytännöt

Lokienhallintamme perustuu viitearkkitehtuuriin ja sen periaatteisiin. Viitearkkitehtuurin avulla varmistamme, että määrittelemme, tuotamme ja hallinnoimme lokeja ja lokitietoja yhteneväällä tavalla. Yhtenäiset lokienhallintakäytännöt myös varmistavat lokeihin liittyvien vaatimusten hallinnan ja soveltamisen osana turvallisuuden johtamisjärjestelmäämme. Lokienhallinnan viitearkkitehtuuri täyttää kansallisen lainsäädännön ja ISO 27001-standardin sekä kansallisen turvallisuusauditointikriteeristön eli Katakriin 2020 vaatimukset. Lisäksi siinä on huomioitu Tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvaluusääädösten soveltamisesta annetut ja todetut lokien hallintaan kuuluvat tehtävät.

Olemme edistäneet vuonna 2021 lokienhallinnan viitearkkitehtuurin mukaisen lokienhallintaratkaisun kehittämistä. Lokienhallinta on olennainen osa riskienhallintaa sekä tietoturvan ja tietosuojan toteutumista. Kehitystyön rinnalla olemme tuottaneet viitearkkitehtuuria täydentäviä ohjeita, joiden avulla yhtenäistämme lokitietojen tuottamista. Lisäksi olemme selvittäneet kehitystyössä olevien tietojärjestelmien lokiratkaisujen vaatimuksenmukaisuutta ja tehneet poikkeamien osalta riskiarviointia.

Tunnistettuihin riskeihin määritetyt hallintakeinot otetaan jatkossa huomioon lokienhallintaratkaisun ja siihen liittyvän ohjeistuksen kehitystyössä.

Olemme määritelleet viraston lokitietoihin liittyvät käsittelytoimet vastuineen ja käynnistäneet näiden prosessien sekä lokitietotarpeiden dokumentoinnin. Toteutamme lokitietopyyntöjen käsittelyn yhtenäistämisen niin, että lokitietojen muuttumattomuus ja eheys voidaan jälkikäteen todentaa.

3.4 Käyttövaltuuksien hallintaa kehitetään edelleen

Tiedonhallintalaki edellyttää, että tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina. Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtioneuvostossa (2019/1101) säädetään, että TL IV -tason tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnustetaan riittävän luotettavasti.

Ylläpidämme luetteloa tietojärjestelmistä, joiden käyttöoikeuksien määrittelystä vastaamme. Tiedonhallintamallin kautta saamme ajantasaisen tiedon tietojärjestelmässä käsiteltävien

tietojen luokittelusta. Tulemme käynnistämään arvioinnin siitä, mitkä käyttövaltuuksien ja pääsynhallinnan vaatimukset tietojärjestelmien sisältämien tietojen käsittelyyn pitää täyttää.

3.5 TIHALA-kehitystehtävä tunnistaa ja vie käytäntöön tiedonhallintalain vaatimuksia

Olemme käynnistyneet joulukuussa 2019 TIHALA-kehitystehtävän, jonka tavoitteena on kouluttaa ja tuoda toimintatapoihimme tiedonhallintalain vaatimukset siirtymäsäännösten asettamassa aikataulussa. TIHALAssa on toteutettu muunmuassa yllä todetut asiakirjajulkisuuskuvaus ja tiedonhallintamalli.

Lokienhallinnan yhdenmukaistaminen, teknisten rajapintojen tuleva viitearkkitehtuuri ja käyttövaltuuksien hallinnan kehittäminen ovat esimerkkejä siitä, kuinka tiedonhallintalain vaatimusten toteuttaminen toteutuu useissa rinnakaisissa kehitystehtävissä. Niiden myötä varmistamme, että lain vaatimukset on viety ohjeisiin ja menetelmiin siten, että ne limittyvät luonnollisesti jokapäiväiseen tekemiseemme.

4. Kokonaisturvallisuuden hallintamalli tukee johtamista

Traficomın Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Se toimii myös kansallisena yhteyspisteenä kyberhäiriöissä, tuottaa tietoturvallisuuden yhdistettyä tilannekuvaa ja viestii tietoturvaan liittyvistä ajankohtaisista ilmiöistä sekä viestintäverkkojen ja -palveluiden toimivuudesta.

Kyberturvallisuuskeskuksen ylijohdaja **Sauli Pahlman**, mikä on kokonaisturvallisuuden hallintamallin merkitys toiminnassanne?

Tiedon ja datan merkitys korostuu toiminnassamme. Tuotamme Kyberturvallisuuskeskuksessa kyberturvallisuuden yhdistettyä tilannekuvaa eli toimimme tietovirtojen keskiönä. Olemme tietoturvaloukkauksia koova kansallinen yhteyspiste, havainnoimme kyberturvallisuuden toimintakenttää ja muutoksia järjestelmillämme. Lopulta analysoimme tiedon erilaisiksi tilannekuvatuotteiksi. Välitämme vuosittain satoja tuhansia kyberturvallisuustapahtumia ja julkaisemme satoja tilannekuvatuotteita päätöksenteon tueksi. Hyödynnämme keräämäämme tietoa myös sääntelytoiminnassamme.

Kokonaisturvallisuuden hallintamalli mahdollistaa Traficomın ja sen Kyberturvallisuuskeskuksen turvallisuuteen ja tietosuojaan liittyvän riskienhallinnan. Ilman tilanne- ja kokonaiskuvaa emme pystyisi johtoryhmässä tai osaamisalueilla arvioimaan analyttisesti riskejä emmekä päättämään etenemisestä.



Psykologinen

Turvallisuuskulttuurimme rakentuu meistä jokaisesta. Riskipohjainen ajattelutapa ohjaa toimintaamme.



Digitaalinen

Turvallisuuden digitaalisella tasolla varmistamme sähköisten palveluidemme ja tietojemme luottamuksellisuuden, eheyden ja saatavuuden.



Fyysinen

Fyysisellä tasolla suojaamme henkilöstömme, toimitilamme ja konesalimme erilaisilta häiriö- ja uhkatilanteilta ja varmistamme toimintakykymme myös poikkeusoloissa.

Turvallisuuskulttuuri rakentuu psykologisesta, digitaalisesta ja fyysisestä tasosta

Turvallisuuskulttuurin eri tasoja ei mielestäni voida erottaa. Jos yksi taso pettää, niin riski realisoituu nopeasti muillakin tasoilla. Jokainen taso vaatii jatkuvaa kehittämistä muuttuvissa uhkatilanteissa. Meidän pitää kehittää tasoja vastaamaan jatkossa paremmin myös osaamisalueiden erityistarpeita. Tasot näkyvät meidän jokaisen päivittäisessä työssä: toimintoihin ei pääse ilman kulkuoikeuksia, työasemat päivittyvät säännöllisesti, tunnistamme aktiivisesti riskejä ja hyötyjä sekä raportoimme näistä tarvittaessa. Turvallisuuskulttuuri ja hallintamalli osaltaan mahdollistavat sen, että voimme tehdä päätöksiä osana tiimien, yksiköiden ja palvelukokonaisuuksien päivittäistä toimintaa.

Kyberturvallisuus vaatii uutta osaamista ja ukiin varautumista

Säätelyn ulottuminen uusiin teknologioihin ja uusille toimialoille jatkuu. Kansainvälinen turvallisuustilanne tulee heijastumaan myös teknologiaan. Yhteiskunnan varautumisen pitää olla verkkojen ja digitaalisten palveluiden osalta kunnossa kaikkialla – valtionhallinnossa, muualla julkishallinnossa ja yksityisellä sektorilla. Digitaitojen ylläpitämiseen ja osaamisvelan syntymisen ennaltaehkäisyyn pitää panostaa Suomessa ja EU:ssa entistä enemmän. Kyberturvallisuuden osaamistarve jatkaa kasvuaan Euroopassa ja Kyberturvallisuuskeskuksessa pyrimme osaltamme ennaltaehkäisemään osaamistyhjiöiden syntymistä. Kyberhäiriöt ulottuvat edelleen uusille toimialoille ja sellaiseen teknologiaan, joka on ollut aiemmin niiltä suojassa. Uusia uhkia syntyy jatkuvasti ja niihin vastataan, mutta perinteiset kyberriskit, kuten palvelunestohyökkäykset ja kiristyshaittaohjelmat ovat jatkossakin varteenotettavia uhkia, joihin tulee varautua. Kansallisesti meidän täytyy pitää huolta siitä, että kansainväliset tietoliikenneyhteydet ovat toimivia ja hyvin varmistettuja.

5. Kyberturvallisuuskeskuksen vuosi 2021 lukuina

Digitaalinen kehitys tuo meille jatkuvasti uusia palveluita. Se parantaa ja helpottaa arkeamme sekä luo uusia ratkaisuja globaalien haasteiden ratkaisemiseen. Tämä kehitys on pääasiassa positiivista. Kehityksen varjopuolena on alati kasvava kyberrikollisuus sekä erilaiset häiriöt.

Kuten kaikille digitaalisille ilmiölle, myös kyberuhkille on luonteenomaista nopea kehitys. Kyberturvallisuuteen liittyvät ilmiöt ovat usein monimutkaisia eivätkä ne noudata ennalta määritettyjä viranomaisvastuita. Suomea koskevien kyberhäiriöiden tai niitä ennakoivien trendien tunnistaminen edellyttää meiltä jatkuvan toimintakyvyn varmistavaa uudistumista sekä kykyä käsitellä turvallisesti valtavia tietomassoja.

Käsitlemme Kyberturvallisuuskeskuksessamme vuosittain miljoonia yksittäisiä tietoturvatapahtumia, häiriöitä ja uutisia, joiden tuottaman tiedon pohjalta tuotamme uutisia kansalaisille, viranomaisille ja organisaatioille sekä kyberturvallisuuden tilannekuvaa ja autamme tietoturvaloukkauksissa sekä ennaltaehkäisemme niitä.

Vuosi 2021 lukujen valossa:

**Tiedotteet verkkosivuillamme:
83**

**Käsitellyt tapaukset:
17 572**

**Verkkohäiriöt:
73**

**Automaattisen tapauskäsittelyn
käsittelemät tapaukset:
209 237**

6. Tietovirtakuvaukset ja toiminnan tunnuslukuja

Luovutukset liikenneasioiden rekisteristä:

Julkiset rekisteritietopalvelut
2 200 000 yksittäiskyselyä

Kuljettajatiedot
25 000 kyselyä

**Ajoneuvon omistaja-
ja historiatiedot**
296 000 kyselyä

**Ajoneuvon
rekisteri- ja verotiedot**
1 800 000 kyselyä

Rajapinnat (API)
106 milj. tietoyksikköä

Aineistot
690 milj. tietoyksikköä

Osoitejälleenmyynti
14,3 milj. tietoyksikköä

Markkinatieto
8,3 milj. tietoyksikköä

Avoin data*
2 366 tietolatausta

*Avoimen datan luku sisältää vuoden 2021 osalta
vain 1-7 kuukaudet johtuen toimittajanvaihdoksesta.

Tietojen luovuttamisen rajoittaminen liikenneasioiden rekisteristä

Luonnollisella henkilöllä on oikeus kieltää henkilötietojensa luovuttaminen:

- Avoimen rajapinnan kautta
- Liikenteeseen liittyviin tarkoituksiin
- Kehittämisen- ja innovaatiotoimintaan

Lisäksi luonnollisella henkilöllä on oikeus kieltää yhteystietojensa luovuttaminen yksittäisluovutuksena.

Oikeushenkilöllä on oikeus kieltää tietojensa luovuttaminen:

- Kehitys- ja innovaatiotoimintaan



Turvakiellosta säädetään väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 36 ja 37 §:ssä. Luovutusrajoitus laajennetaan kattamaan myös luonnollisen henkilön nimi, kun turvakielto siirretään liikenneasioiden rekisteriin.

Tiedonluovutusrajoitukset eivät estä tiedon luovuttamista viranomaiselle tai lakisääteisen tehtävän suorittamiseen.

Vuonna 2021 liikenneasioiden rekisterissä noin 453 213 henkilöllä oli voimassa jokin tiedonluovutuskielto. Yhdellä henkilöllä voi olla voimassa useampi kieltoaji samanaikaisesti. Yritykset ja yhteisöt eivät voi rajoittaa tietojensa luovutusta muuhun kuin kehitys- ja innovaatiotoimintaan. Turvakieltoa haetaan Digi- ja väestötietovirastosta sen ylläpitämään väestötietojärjestelmään (VTJ). Käytetyin tiedonluovutuskieltoaji on suoramarkkinointikielto, joka estää henkilötietojen luovuttamisen suoramarkkinointia varten. Tämä estää markkinointipostin esimerkiksi katsastusyrittäksiltä tai autoliikkeiltä.

Traficom on palveleva liikenteen ja viestinnän lupa-, rekisteri- ja valvontaviranomainen. Näiden tehtävien hoitaminen edellyttää kattavaa tietopääomaa, joka koostuu laajoista viestinnän, liikenteen ja liikkumisen tietovarannoista. Seuraavassa on kuvattu tarkemmin keskeisten rekisteriemme ja tietovarantojemme tietovirrat. Tietovirtakuvauksissa on kuvattu tietoja säännönmukaisesti luovuttavat tahot, tietojen säilytys sekä tahot, joille tietoja säännönmukaisesti luovutetaan. Kuvausten sisältämät keskeiset tunnusluvut antavat käsityksen tietovarantojen volyymeistä.

Liikenneasioiden rekisteri – tiedon lähteet

Liikenneasioiden rekisteriin tulee tietoa seuraavilta tahoilta:

- Luvan hakijalta ja/tai haltijalta
- Ilmoituksenvaraista toimintaa harjoittavalta liikennevälineen omistajalta, haltijalta ja/tai käyttäjältä
- Liikennevälineen ja sen moottorin valmistajalta ja/tai maahantuojalta/edustajalta
- Oppilaitokselta, kouluttajalta ja näytön vastaanottajalta
- Lääkäriltä ja psykologilta sekä sairaanhoito- tai terveydenhuoltotoimintaa harjoittavalta yhteisöltä ja/tai laitokselta
- Lupakirjan ja kortin valmistajalta ja/tai käsittelijältä
- Suomen ja Venäjän välistä rautatieyhdyshä liikennettä harjoittavalta rekisteröintitehtäviä suorittavalta katsastustoiminnan harjoittajalta
- Yksittäishyväksyntöjä myöntävältä Traficomin sopimuskumppanilta
- Liikennevakuutuskeskukselta
- Vakuutusyhtiöltä
- Laivaisännältä ja varustamolta
- Toiselta viranomaiselta



Liikenneasioiden rekisteriin tallennettavat tiedot ja niiden säilytysaika

Henkilön tiedot:

- Henkilötunnus
- Sukupuoli
- Syntymäaika (jos ei ole henkilötunnusta)
- Kansalaisuus
- Kotikunta
- Nimi
- Nimikirjoitusnäyte
- Osoite tai muu yhteystieto
- Syntymäaika, -kunta ja -valtio
- Tieto henkilön kuolemasta
- Valokuva
- Yritys- ja yhteisötunnus
- Äidinkieli ja asiointikieli
- Lakisääteiset maksut
- Verot ja niiden suorittaminen
- Suomalaisessa aluksessa työskentelevien henkilöiden merimiestoimet
- Takavarikot
- Tieliikenteen valvontalaitteiden korttitiedot
- Ulosotot
- Vakuustakavarikot
- Vakuutukset
- Vammaisen pysäköintiluvat
- Myönnetyt luvat tai sen peruuttaminen
- Velkajärjestelyt
- Kiinnitykset
- Ajokiellot ja muut vastaavat seuraamukset
- Rikoksista seuranneet rangaistukset
- Tehdyt rikokset, joiden valvontatehtävien johdosta määritellyt seuraamukset

Organisaation tiedot:

- Aputoiminimi
- Asiointikieli
- Kotipaikka
- Nimi
- Osoite ja muu yhteystieto
- Tieto muun yhteisön vastuuhenkilöstä
- Tieto vastuuhenkilöiden yksilöinti- ja yhteystiedoista
- Toimitusjohtaja
- Vastuunalainen yhtiömies
- Yhtiön omistussuhteet
- Yritys- ja yhteisötunnus
- Kiinnitystieto
- Konkurssitieto
- Lakisääteinen maksutieto
- Verotieto ja sen suorittamistieto
- Suomalaisessa aluksessa työskentelevien henkilöiden merimiestoimitiedot
- Takavarikkotieto
- Tieliikenteen valvontalaitteiden korttitieto
- Ulosottotieto
- Vakuustakavarikkotieto
- Vakuutustieto
- Velkajärjestelytieto
- Yrityssaneeraustieto

Säilytysaika 10 vuotta:

Henkilötiedot:

Liikennevälineen romuttaminen
Henkilön kuolema
Rekisteröidylle asetettu toimintakielto tai muu Liikenne- ja viestintäviraston tai poliisin tekemää hallinnollista toimenpidettä koskeva tieto

Säilytysaika 5 vuotta:

Henkilötiedot:

Virheelliseksi todettu ja merkitty tieto

Tiedot, jotka poistetaan heti kun ne käyvät tarpeettomiksi:

Rikos- ja riketiedot
Rekisteröidyn terveydentilaa koskevat tiedot

Liikenneasioiden rekisteriin tallennettavat tiedot ja niiden säilytysaika

Liikennevälinetiedot:

- Anastustieto
- Hallintatieto
- Haltijatieto
- Historiatieto
- Hyväksyntätieto
- Katsastustieto
- Kaupallinen tieto
- Kunnossapidosta vastaava taho
- Kunnossapitoa koskeva tieto
- Käyttäjätieto
- Käyttökieltoa koskeva tieto
- Käyttörajoitusta koskeva tieto
- Käyttötarkoitustieto
- Käyttöönottotieto
- Käytöstä poistotieto
- Luokitustieto
- Muu rekisteröintitieto
- Muu teknistä tarkastusta koskeva tieto
- Omistajatieto
- Rakennustieto
- Rekisteritunnus ja muu yksilöinti- ja numerointitieto
- Tekninen tieto
- Tieto kotipaikasta ja käyttöalueesta
- Tieto viranomaistarkastuksesta
- Väliaikaista käyttöä koskeva tieto

Säilytysaika:

- Liikennevälinetiedot säilytetään pysyvästi

Henkilölupatiedot:

- Tieto myönnetystä tai peruutetusta luvasta
- Lupaehdot
- Luvan erivapaudet
- Luvan muutokset
- Evätty lupahakemus
- Luvan myöntäjä ja sijaintivaltio
- Luvan, kelpoisuuden, hyväksynnän tai pätevyuden hakeminen ja käsittely
- Koulutukset ja kokemus
- Kokeista ja arvioinneista tarvittava kielitaito
- Terveystila ja tieto lääkärin ja psykologin tarkastuksista
- Lupien, kelpoisuuksien, hyväksyntöjen ja pätevyksiä vastaavien korttien, kirjojen ja todistusten myöntäminen, peruuttaminen, katoaminen ja tuhoutuminen
- Muut Euroopan unionin lainsäädännön ja kv-sopimuksien mukaan liikenteen viranomaisen rekistereihin kirjattavat tiedot

Säilytysaika 10 vuotta:

- Luvan päättymisestä tai kun henkilötieto on tullut käyttötarkoitukseensa nähden tarpeettomaksi
- Raideliikenteen kelpoisuustiedot luvan päättymisen jälkeen

Säilytysaika 70 vuotta:

- Merimiesten meripalvelu-, koulutus- ja pätevyystiedot tiedon rekisteröinnistä

Organisaatiolupatiedot:

- Hyvämaineisuuden ja luotettavuuden arviointiin liittyvät tiedot
- Ilmoituksen käsittelyä koskevat tiedot
- Ilmoituksenvaraista toimintaa koskevat tiedot
- Tiedot luvan sisällöstä
- Tiedot lupaehdoista
- Tiedot lupatunnuksesta
- Luvan hakemista ja sen käsittelyä koskevat tiedot
- Tiedot luvan muutoksesta
- Tiedot luvan myöntämisen ja ilmoituksenvaraiseen toimintaan liittyvän rekisterimerkinnän tekemisen edellytyksistä
- Tieto luvan voimassaoloajasta
- Myönnetty lupa tai sen peruuttaminen
- Poikkeamailmoitustiedot
- Riskiyritystieto

Säilytysaika:

- 6 vuotta luvan peruuttamisesta tai päättymisestä

Tietojen luovuttaminen liikenneasioiden rekisteristä

Yleisesti saatavilla olevat tiedot:

- Voimassa olevat toiminnanharjoittajaluvat
- Luvan yksilöintitunnus
- Luvan haltijan nimi
- Toiminnanharjoittamiseen liittyvät yhteystiedot
- Ilmoituksenvaraisen toiminnan osalta vastaavat tiedot

Tiedot voidaan luovuttaa siten, että tiedot eivät ole yhdistettävissä luonnollisiin henkilöihin ja oikeushenkilöihin.



Jokaisella on oikeus yksittäis-luovutuksena saada seuraavat tiedot:

- Yritys- ja yhteisötunnuksen, yrityksen nimen tai lupatunnuksen perusteella
 - » Tiedot toiminnanharjoittajaluvan haltijan nimestä ja yhteystiedoista
 - » Lupatunnuksesta
 - » Luvan voimassaoloajasta
 - » Vastuuhenkilön nimestä
- Luonnollisesta henkilöstä toiminnanharjoittajana etu- ja sukunimen, henkilötunnuksen tai muun yksilöivän tunnuksen perusteella tiedot
 - » Toiminnanharjoittajan nimestä
 - » Työyhteystiedoista
 - » Lupatunnuksesta
 - » Luvan voimassaoloajasta
- Liikennevälineen yksilöivän tunnisteen perusteella
 - » Tiedot liikennevälineestä sekä omistajan ja haltijan, käyttäjän sekä edustajan nimestä sekä osoite- ja muista yhteystiedoista ja katsastustiedoista sekä verotuksesta, kiinnityksestä sekä vakuutuksen ottajasta
 - » Etu- ja sukunimen, henkilötunnuksen tai muun yksilöivän tunnuksen perusteella tiedot henkilön oikeudesta kuljettaa liikennevälinettä tai muusta henkilöluvan voimassaolosta ja laajuudesta.

Liikenteeseen liittyviin tarkoituksiin tietoja saa luovuttaa:

- Liikennepalvelujen tarjoamiseen ja kehittämiseen
- Mieli- ja markkinatutkimukseen, suoramarkkinointiin sekä muuhun osoite- ja tietopalveluun
- Asiakasrekisterin yhteystietojen ja liikennevälineen tietojen päivittämiseen
- Muihin vastaaviin rekisterinpitäjän hyväksymiin tarkoituksiin.

Luovutettuja tietoja saa käyttää vain siihen käyttötarkoitukseen, johon ne on luovutettu. Tietoja saa luovuttaa edelleen tai muuten antaa sivulliselle vain, jos siitä on säädetty laissa, luovutus perustuu Suomea sitovaan kansainvälisen sopimuksen veloitteeseen tai Euroopan Unionin lainsäädäntöön, tai jos Liikenne- ja viestintävirasto on antanut siihen luvan.

Kehittämisen- ja innovaatiotoimintaa varten voidaan luovuttaa yksittäistapauksissa tietoja:

- Liikennejärjestelmän ja palvelujen kehittämiseen ja tarjoamiseen
- Liikennejärjestelmää ja palveluita koskevan tietoisuuden ja ymmärryksen lisäämiseen
- Liikenneturvallisuuden parantamiseen ja liikenteen ympäristötavoitteiden saavuttamisen edistämiseen.

Salassa pidettäviä tietoja saa luovuttaa ainoastaan henkilön suostumuksella tai sellaisessa muodossa, että niitä ei voida yhdistää yksittäiseen henkilöön.

Traficomien saamia tietoja rikos- tai sakkorekisteristä saa luovuttaa ainoastaan sellaisessa muodossa, että niitä ei voida yhdistää yksittäiseen henkilöön. Luovutettuja tietoja saa käyttää vain siihen käyttötarkoitukseen, johon ne on luovutettu. Tiedot on poistettava heti, kun ne eivät enää ole tarpeen käyttötarkoitusta varten. Tietoja ei saa luovuttaa edelleen.

Toiselle viranomaiselle tai muulle laissa säädettyä tehtävää hoitavalle salassapitosäännösten estämättä voidaan antaa sellaisia tietoja, jotka ovat välttämättömiä sille laissa säädettyjen tehtävien hoitamiseksi:

Virastomme ei saa kuitenkaan luovuttaa sellaisia salassa pidettäviä tietoja, joita olemme saaneet rikos- tai sakkorekisteristä, ellei muualla laissa ole toisin säädetty.

Saamme luovuttaa rekisteristä tietoja ulkomaan viranomaisille tai viranomaistehtäviä varten, jos luovuttaminen perustuu lakiin, Euroopan yhteisön lainsäädäntöön tai Suomea sitovaan kansainvälisen sopimuksen velvoitteeseen. Jos henkilötietoja siirretään ETA-alueen ulkopuolelle, Euroopan unionin yleisen tietosuojasetuksen V-luvun edellytysten on täyttyttävä.

Liikenneasioiden rekisteristä tietoja saanut muu viranomainen saa luovuttaa tietoja edelleen samojen edellytysten täytyessä.

Lisäksi saamme luovuttaa valokuvan ja nimikirjoitusnäytteen palveluntarjoajalle, joka tarvitsee sen laissa säädettyä tehtäväänsä varten.



Viestinnän tietoineistot

Viestintäverkkoihin liittyviin tietoineistoihin tulee tietoja seuraavilta tahoilta:

- Teleyritykset
- Viestintäpalvelujen tarjoajat
- Radioluvan hakijat
- Traficom
- Teleyritykset
- Havaintoilmoituksen tehneet tahot tai henkilöt
- Teleoperaattorit ja muut verkko-operaattorit
- Radiohäiriöilmoituksen tekijät

Tiedot talletetaan seuraaviin tietoineistoihin:

- Laajakaistaverkkojen saatavuustiedot
- Luvanvaraisten radioverkkojen tiedot
- Julkinen taajuusjakotaulukko
- Tv- ja radioasemat Suomessa
- Tietoturvaloukkaushavainnot
- Havainnointi- ja varoitusjärjestelmän tiedot
- Teleyritysten ilmoittamat Tietoturvaloukkaushavainnot
- Viestintäverkkojen viat ja häiriöt
- Radiohäiriöt
- Tiedot toimialan kehityksestä

Tietojen käyttötarkoituksia ovat:

- Viestintämarkkinoiden ohjaus- ja valvontatehtävät
- Monitori-palvelu
- Taajuuksien käyttöä koskevat ohjaus- ja valvontatehtävät
- Radiomikrofonisovellus
- Avoimen datan aineisto
- Viestintäverkkojen ja -palvelujen toimivuuden ja turvallisuuden valvonta
- Neuvonta
- Taajuuksien käytön valvonta ja radiohäiriöiden selvittäminen
- Tiedon julkaisu



Viestinnän tietoaineistot

Viestinnän henkilölupiin, kelpoisuuksiin ja henkilöille myönnettyihin tunnuksiin tietoja tulee seuraavilta tahoilta:

- Tutkintoihin osallistujat
- Tutkintojen vastaanottajat
- Todistusten hakijat
- Suomen Radioamatööriliitto (SRAL)
- Radioluvan hakijat
- Traficom
- Verkkotunnusvälittäjät

Tiedot talletetaan seuraaviin tietoaineistoihin:

- Merenkulun radioviestinnän pätevyystodistukset
- Radioamatöörien pätevyystodistukset
- Yksityishenkilöille myönnetyt radioluvat
- Radioamatöörien radioluvat
- Radioamatöörien kutsumerkit
- Alusten meriradionumerot
- Fi-verkkotunnusten tiedot

Tietojen käyttötarkoituksia ovat:

- Taajuuksien käyttöä koskevat ohjaus- ja valvontatehtävät
- Avoimen datan aineisto
- Rekisterin ylläpitotehtävä

Viestinnän tietoineistot

Toiminnanharjoittajiin ja toiminnanharjoittajille myönnettyihin tunnuksiin liittyviä tietoja tulee seuraavilta tahoilta:

- Puhelinnumeroiden, koodien ja tunnusten hakijat
- Radioluvan hakijat
- Toimilupien hakijat
- Traficom
- Teletoimintailmoituksen tehneet
- Ohjelmistotoimintailmoituksen tehneet toimijat
- Tilausohjelmapalveluilmoituksen tehneet toimijat
- Maksutelevisiopalveluilmoituksen tehneet toimijat
- Ilmoituksen tehneet toimijat
- Postitoimintailmoituksen tehneet toimijat
- Verkkotunnusvälittäjäksi ilmoittautuneet

Tiedot talletetaan seuraaviin tietoineistoihin:

- Televerkkoihin liittyvien puhelinnumeroiden, koodien ja tunnusten haltijat
- Radioluvan haltijat
- Toimiluvan haltijat
- Puhelin- tai laajakaistaliittymän tarjontaan velvolliset yleispalveluyritykset
- Teletoiminnan harjoittajat
- Ohjelmistotoiminnan harjoittajat
- Tilausohjelmapalvelun tarjoajat
- Maksutelevisiopalvelun tarjoajat
- Hyväksytyt sähköisten luottamuspalvelujen tarjoajat
- Vahvan sähköisen tunnistautumispalveluntarjoajat
- Postitoiminnan harjoittajat
- Fi-verkkotunnusvälittäjät

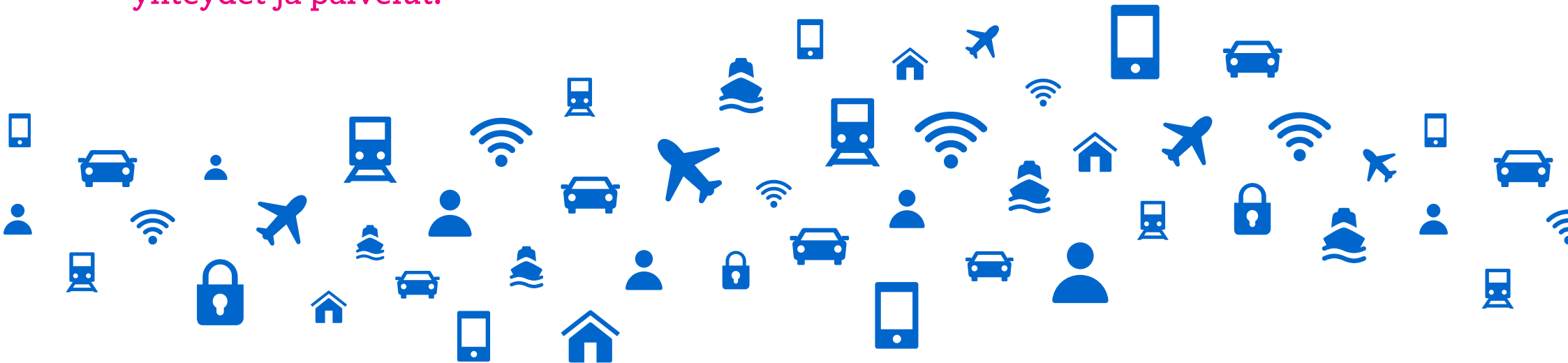
Tietojen käyttötarkoituksia ovat:

- Rekisterin ylläpitotehtävä
- Osittain avoimen datan aineisto
- Taajuuksien käytön ohjaus- ja valvontatehtävät
- Yleispalvelun valvontatehtävät
- Verkkotunnustoiminnan ohjaus- ja valvontatehtävä

Palveluiden tunnuslukuja 2021

• Ajoneuvot liikennekäytössä	5,2 milj.	• Ilmailun lupakirjat	7 060
• Ajokortit	3,8 milj.	• Fi-verkkotunnukset	526 000
• Merenkulun pätevyudet	6 200	• Ajoneuvojen rekisteröintitapahtumat	5,7 milj.
• Rautatiekalusto	10 800	• Neuvontatapahtumat	0,76 milj.
• Rautateiden kelpoisuudet	2 300	• Sähköiset asiointitapahtumat	8 milj.
• Suoritetut kuljettajan tutkinnot	112 600	• Kauppalaivat	1 235
• Ilma-alukset	1 460	• Radiolupien taajuudenannot	111 000

”Varmistamme liikenteen ja viestinnän toimivat ja turvalliset yhteydet ja palvelut.



TRAFICOM

Liikenne- ja viestintävirasto

Liikenne- ja viestintävirasto Traficom

PL 320, 00059 TRAFICOM

p. 029 534 5000

traficom.fi