Tietotilinpäätös 2021

Sisällysluettelo

1 Johdanto 3
Yleiskatsaus ja tilannearvio 3
1.1 Tietosuojan tilanne 3
1.2 Tietoturvan tilanne 4
1.3 Tiedonhallinnan tilanne 4
2 Tiedonhallinta Kevassa 5
2.1 Minkälaista tietoa Kevassa käsitellään? 6
2.2 Julkisuusperiaatteen toteutuminen 7
2.3 Robotiikan käyttö Kevassa 8
3 Kevaan kohdistuvat tietoriskit 8
4 Tietosuojan toteutuminen Kevassa 9
4.1 Kevan henkilötietojen käsittelyperusteet ja rekisteröityjen oikeudet 9
4.2 Toimenpide- ja kehittämistarpeet 11
4.3 Tietosuojatapahtumat ja -herätteet 11
5 Tietoturvallisuuden toteutuminen Kevassa 12
5.1 Lokipolitiikka 14
6 Lopuksi 15

1 Johdanto

Kevassa huolehditaan lakisääteisistä tehtävistä eli kunta-alan, valtion, kirkon, Kelan henkilöstön ja Suomen Pankin eläketurvasta sekä tarjotaan työelämäpalveluita työurien tukemiseksi. Henkilöasiakkaita on noin 1,3 miljoonaa ja työnantaja-asiakkaita noin 2000. Näin ollen Kevassa kerätään ja käsitellään paljon eritasoista henkilötietoa. Henkilötiedon määritelmä on hyvin laaja ja tarkoittaa kaikkea tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvää tietoa.

Yleisen tietosuoja-asetuksen mukaisena vastuullisena rekisterinpitäjänä Keva vastaa siitä, että yleisen tietosuoja-asetuksen vaatimuksia ja periaatteita henkilötietojen käsittelystä noudatetaan ja vaatimustenmukaisuus on kyettävä osoittamaan. Tietotilinpäätös on yksi keino täyttää yleisen tietosuoja-asetuksen mukainen osoitusvelvollisuus. Kyseessä on vapaamuotoinen raportti, jossa voidaan kartoittaa henkilötietojen käsittelyä koskevat keskeiset seikat organisaatiossa. Raporttia voidaan osoitusvelvollisuuden lisäksi käyttää muun muassa tietojohtamisen, compliancen, riskienhallinnan ja sisäisen tarkastuksen apuvälineenä. Raportin sisältö muotoutuu kunkin organisaation tiedontarpeiden mukaan. Koska Kevassa käsitellään paljon toiminnan luonteen vuoksi vakuutettujen ja muiden asiakkaiden henkilötietoja, vastuullisuus ja läpinäkyvyys henkilötietojen käsittelyssä korostuvat. Lisäksi tavoitteena on tukea tietosuojatyön tekemistä ja sen vaikuttavuutta. Parhaimmillaan tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn.

Kevassa laaditaan jatkossa tietotilinpäätös vuosittain ja se tulee sisältämään vuosittain raportoitavia asioita, kuten tietosuoja- ja tietoturvatapahtumat. Eri vuosina voidaan kuitenkin organisaation tarpeista riippuen keskittyä tiettyihin osakokonaisuuksiin. Vuoden 2021 osalta kartoitetaan hieman tarkemmin tietojenkäsittelyyn liittyvää robotiikkaa ja sen käyttöä.

Tietosuojavastaava esittää suuret kiitokset kaikille, jotka ovat antaneet tietoja ja avustaneet tämän tilinpäätöksen laatimisessa.

Yleiskatsaus ja tilannearvio

1.1 Tietosuojan tilanne

Tietosuojatyön tekeminen on jatkunut vakaana Kevassa. Tietosuoja-asioihin kiinnitetään huomiota ja mahdollisiin poikkeamiin reagoidaan ja ne otetaan vakavasti. Tietosuojavastaavan yhteistyö eri yksiköiden on sujunut hyvin, tiettyjen toimintojen osalta yhteydenpitoa on enemmän kuin toisien, riippuen toimintojen luonteesta. Eläkeasiaoissa käsitellään runsaasti henkilöasiakkaiden tietoja, joiden osalta tietosuojaseikat korostuvat. Sen sijaan esimerkiksi sijoitustoiminnossa yleensä ottaen henkilötietojen käsittely on vähäisempää. Voidaan todeta, että koko talon tasolla tietosuojaongelmiin on reagoitu pikaisesti ja tehty asiaankuuluvat korjaavat toimenpiteet.

Tietosuojan osalta toiminnan kehittäminen on jatkuvaa. Tietosuojalainsäädäntö ja erityisesti siihen liittyvä oikeus- ja tulkintakäytäntö muokkaa työn tekemistä, myös käytännön tasolla. Lisäksi sääntelyn ylikansallinen luonne tarkoittaa, että on seurattava oikeuskäytäntöä myös Euroopan unionin ja sen jäsenmaiden tasolla. Viime vuoden tietotilinpäätöksen kehityskohteisiin tartuttiin ja työ jatkuu myös 2022. Voidaan sanoa, ettei tietosuojavastaavan työ

ole koskaan valmis, vaan aina voidaan tietosuoja-asioissa parantaa ja kehittää prosesseja tarkoituksenmukaiseksi.

Kevassa aloitettiin vuonna 2020 pilveistämisstrategian valmistelu alkukartoituksella, joka valmistui huhtikuussa 2021. Elokuussa 2021 pilveistämistyö jatkui vaiheella 2 - suunnittelu. Suunnitteluvaiheen lopputuotoksena syntyi pilveistämisen etenemissuunnitelma, master plan, jonka mukaisesti vaiheeseessa 3 Kevan järjestelmien pilveistäminen tullaan tekemään. Suunnitteluvaiheessa tunnistettiin myös tarve jatkaa hybridi-ympäristöllä toistaiseksi. Kevan järjestelmät ja palvelut tuotetaan jatkossakin yksityisestä pilvestä Suomessa sekä julkipilvestä ETA-alueella. Vaihe 2 - suunnittelu päättyi toukokuussa 2022.

Pilvipalveluihin siirtymisessä on huomioitava myös juridisia kysymyksiä tietosuojan näkökulmasta liittyen mahdollisiin tiedonsiirtoihin ETA-alueen ulkopuolelle.

1.2 Tietoturvan tilanne

Kevan tietoturvaan on panostettu merkittävästi viimeisten vuosien aikana. Vuonna 2021 kilpailutimme CSOC toimittajan, jonka tehtävänä on valvoa 24/7 Kevan tietoturvatapahtumia ja reagoida niihin tarvittaessa. Sovimme samassa yhteydessä eskalointimenettelyn, jolla CSOC-kumppani välittää kriittiset tietoturvatapahtumat välittömästi myös Kevan muille palvelutoimittajille toimenpiteitä varten.

Salasanojen laatuun panostettiin ottamalla käyttöön huonojen salasanojen esto. Vaihdettavaksi annettua salasanaa verrataan Microsoftin ylläpitämään listaan, jota on täydennetty suomalaisilla kuukausilla ja viikonpäivillä. Muutimme myös eräiden palvelutunnusten salasanojen käyttöä siten, että ne haetaan keskitetystä salasanavarastosta sen sijaan, että salasanat olisivat asetustiedostoissa selväkielisinä.

Keva on jatkanut henkilöstön kouluttamista sähköpostin kautta tulleiden haittaohjelmien havaitsemiseksi. Käyttäjille lähetetään simuloituja viestejä, jotka mahdollisuuksien mukaan pyrkivät olemaan hyvin samankaltaisia kuin oikeatkin huijausviestit.

Tietoturvaa kehitetään myös jatkuvasti. Uusi keskitetty lokienhallintapalvelu otettiin käyttöön, teimme tietoturvatestauksia järjestelmiimme sekä harjoittelimme kybertilanteen hallintaa yhdessä IT:n, viestinnän ja Kevan johdon kanssa. Tietoturvan ulkoisten sidosryhmien kanssa tehdään jatkuvaa yhteistyötä mm. Microsoft auditoi ympäristömme.

Pilvipalveluiden laajentuvan käytön suunnittelussa tietoturvalla on keskeinen rooli. Pilvipalvelut voidaan ottaa käyttöön tietoturvallisesti vaarantamatta tietosuojaa.

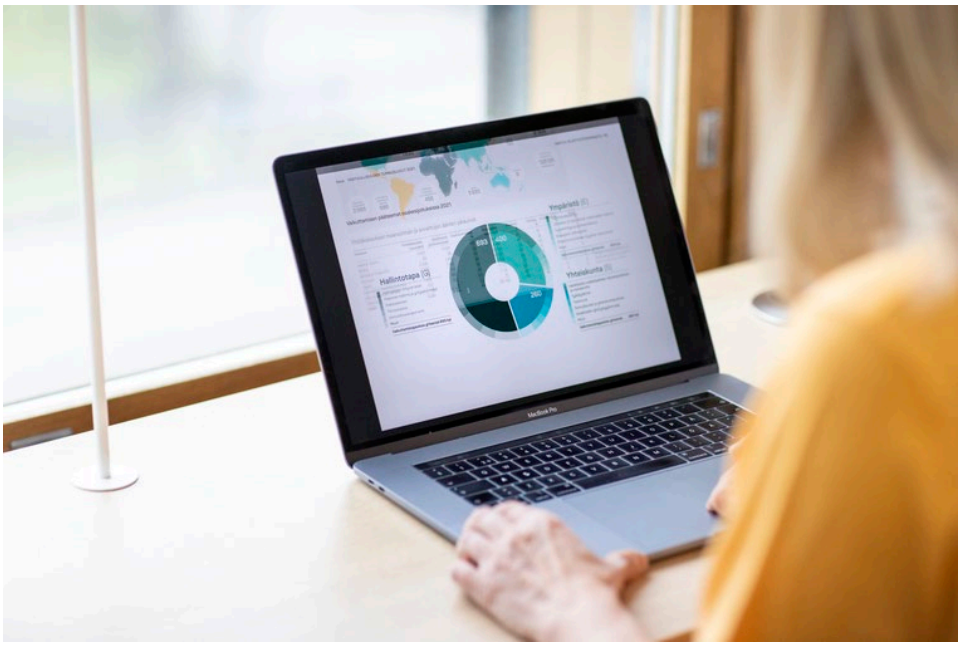
1.3 Tiedonhallinnan tilanne

Tiedonhallinnan osalta vuonna 2021 toteutettiin uuden asianhallinta- ja arkistojärjestelmän (sis. diaari) kilpailuttaminen. Edellinen tietojärjestelmä oli vuodelta 2015. Uuden asianhallintajärjestelmän vaatimuksena oli, että se mahdollistaisi paremmin asiakirjojen elinkaaren seurannan, mikä helpottaa esimerkiksi sopimusten päättymispäivämäärien seuraamista. Uusi järjestelmä

lähettää myös muistutuksia tehtävistä ja siten helpottaa asiakirjojen ajantasaista kirjaamista.

Vuonna 2020 perustettiin Tiedolla johtamisen verkosto, jonka koordinaatioryhmä jatkoi työskentelyään vuonna 2021. Ryhmässä on edustus Kevan jokaisesta toiminnosta ja se koordinoi Kevan tiedolla johtamisen tarpeita ja niihin liittyvää resurssointia sekä pyrkii parantamaan tiedonkulkua varmistamaan strategian mukaisen kehittämisen talotasoisissa tiedolla johtamisen hankkeissa sekä koordinoi näiden etenemistä. Ryhmä edistää myös verkoston jäsenten data- ja analytiikkaosaamista. Vuonna 2021 uutena asiana ryhmä käsitteli tiedolla johtamiseen liittyvien hankkeiden viemistä samalle tiekartalle ensimmäistä kertaa Kevassa.

Kevassa päivitettiin ohjeet sekä järjestettiin koulutusta julkisuuslain mukaisiin tietopyyntöihin vastaamisessa.



2 Tiedonhallinta Kevassa

Kevan tietohallinnon pääperiaatteet ja toimintatavat on dokumentoitu Tiedonhallintapolitiikka-asiakirjaan, joka on hyväksytty johtoryhmässä vuonna 2020. Vuonna 2021 tähän asiakirjaan ei tullut muutoksia. Tietohallintopolitiikan mukaan Kevan tiedonhallintamalli sekä kuvaus asiakirjajulkisuudesta ohjaavat tiedonhallintaa. Tiedonhallintamalli käsittää tiedon koko elinkaaren. IT-yksikkö vastaa tiedonhallintamallin laatimisesta ja ylläpidosta. Asiakirjahallinto on laatinut tiedonhallintalain mukaisen kuvauksen asiakirjajulkisuudesta sekä tiedonohjaussuunnitelman (TOS) sekä ylläpitää niitä. Tiedonhallintamalli, kuvaus asiakirjajulkisuuden toteuttamisesta sekä tiedonohjaussuunnitelma on toteutettu Kevan sisäisenä yhteistyönä.

Asiakirjahallinnossa otettiin vuonna 2018 robotti tuotantokäyttöön. Robotiikasta enemmän luvussa 2.3.

2.1 Minkälaista tietoa Kevassa käsitellään?

Lain mukaan Kevan tehtävänä on hoitaa julkisen alan eläketurvan toimeenpanoa ja henkilöstön työkyvyttömyysriskin vähentämiseen liittyvää toimintaa. Lisäksi Kevan tehtävänä on hoitaa jäsenyhteisöjensä palveluksessa olevan henkilöstön eläketurvan rahoitusta. Kevan pääprosessit jakautuvat näiden tehtävien mukaisesti työnantaja- ja työkykyprosessiin, eläkeprosessiin sekä sijoitusprosessiin. Näiden lisäksi on määritelty toiminnan tukiprosessit sekä johtamisprosessit. Prosessien hoitamiseksi käsitellään tietoa useissa eri tietojärjestelmissä.

Salassa pidettävät ja erityiset henkilötietoryhmät, mm.

- Eläkerekisterin tiedot (sis. laajasti tietoa etuuksista, terveydentilasta, perhesuhteista, taloudellisesta tilanteesta)
- Työnhakijoita ja Kevan työntekijöitä koskevat tiedot (esim. tieto ammattiliitosta)
- Henkilötietoja sisältävät lokitiedot

Salassa pidettävä tieto, mm.

- Liikesalaisuudet (Kevan ja sopimuskumppanien)
- Turvajärjestelyt
- Poikkeusoloihin varautuminen
- Oikeudenkäynnin osapuolena oikeudenkäyntiin valmistautumista koskevat tiedot

Henkilötiedot, mm.

- Vuokraustoimintaan liittyvät tiedot
- Yhteyshenkilöt (työnantajat, sidosryhmät, sopimuskumppanit, sijoitustoiminta)
- Työnhakijoita ja Kevan työntekijöitä koskevat tiedot

Julkinen ja sisäinen tieto

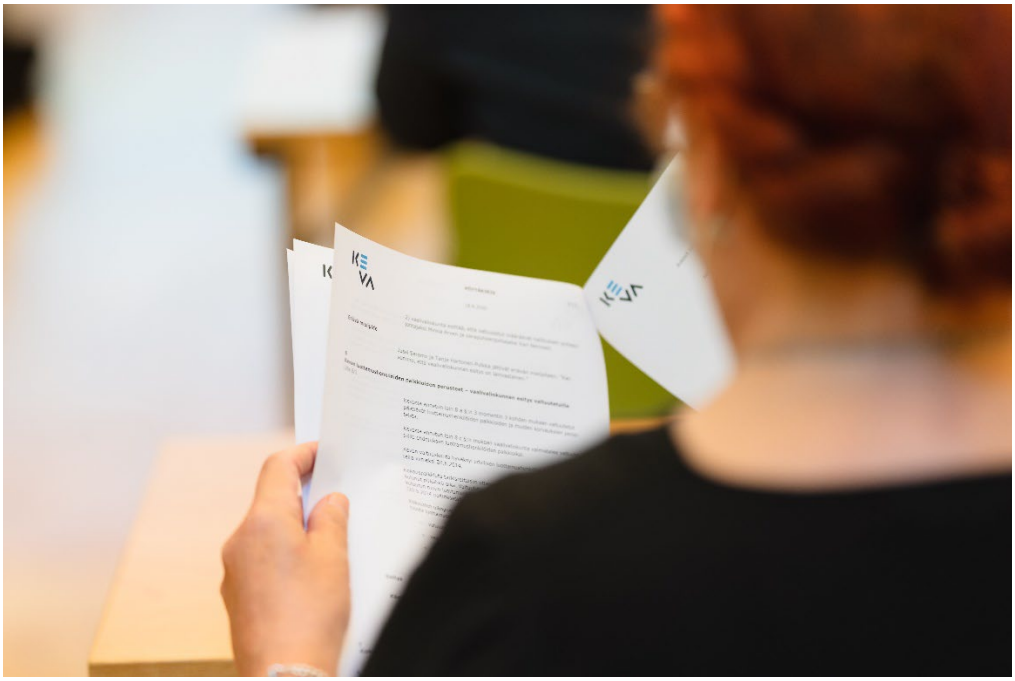
- Viranomaisen asiakirjat (lähtökohtaisesti julkisia)
- Ei-asiakirjat kuten sisäiseen käyttöön hankitut asiakirjat (ei-julkisia)

2.2 Julkisuusperiaatteen toteutuminen

Pääsääntöisesti kaikki Kevan asiakirjat ovat viranomaisten toiminnan julkisuudesta annetun lain (621/1999) nojalla julkisia, jollei julkisuuslaissa tai muussa laissa erikseen toisin säädetä. Eläkeasiakirjat ovat kuitenkin salassa pidettäviä ja muiden asiakirjojen osalta on harkittava tapauskohtaisesti, ovatko ne julkisia vai soveltuuko niihin jokin julkisuuslaissa tai muualla lainsäädännössä oleva salassapitoperuste. Julkisuuslain soveltamiseen on liittynyt käytännön tilanteissa haasteita. Vuonna 2021 järjestettiinkin koulutusta julkisuuslain mukaisiin tietopyyntöihin vastaamisessa ja siihen liittyen julkaistiin sisäisesti päivitetty ohje. Epäselvissä tilanteissa yhteyttä on voinut aina ottaa juridisiin palveluihin, jotka voivat avustaa tietopyyntöihin vastaamisessa, erityisesti pohdinnassa siitä, onko jokin tietty asiakirja julkinen vai ei

Keva vastasi vuonna 2021 oikeusministeriön asettaman työryhmän kyselyyn, jossa kartoitetaan julkisuuslain ajantasaistamistarpeita sekä selvitetään ja arvioidaan julkisuusperiaatteen asianmukaisen toteutumisen ja toteuttamisen ongelmakohtia. Tässä yhteydessä Keva totesi, että suurimmat haasteet lain soveltamiselle ovat julkisuusperiaatteen kannalta salassapitoperusteiden tulkinta sekä tulkinta siitä, mitkä asiakirjat ovat ns. sisäistä tarkoitusta varten, jolloin niihin ei sovelleta julkisuuslakia. Lisäksi henkilötietojen luovuttamista koskevat säännökset kaipaisivat selkeyttämistä.

Vuonna 2021 tehtyjä tietopyyntöjä oli 14 kappaletta, joista kaksi koski lokitietoja. Edellisen vuoden tapaan, useimmin toistuva pyyntö koskee kansanedustajien sopeutumisrahan saajia.



2.3 Robotiikan käyttö Kevassa

Ensimmäinen robottiprosessi otettiin käyttöön Kevassa 2018. Samalla luotiin käyttäjät Roope Robotti tuotantopuolelle ja Roosa Robotti testipuolelle. Myöhemmin otettiin käyttöön toinen tuotantotunnus nimeltä Elmeri Robotti. Kevan robotiikkaprosessit ajetaan Blue Prism -ohjelmistorobotiikkaympäristössä. Robotit ovat käytössä eläke- ja työelämäpalveluissa, sijoitustoiminnossa, rahoituksen ja talouden toiminnossa sekä yleisjohdossa. Roboteilla pyritään vähentämään manuaalityön määrää ja sen myötä tehostamaan toimintaa. Robotit hoitavat tehtäviä, joiden suorittamisessa ihmistyön käyttö ei ole tarkoituksenmukaista, kuten materiaalien siirtämistä järjestelmistä toiseen; todistuspyyntöjen, maksutodistusten tai sopimusmuistutusten automaattista lähettämistä sekä tietojen vertailua eri tarkoituksiin. Poikkeustilanteita syntyy myös robottien toiminnassa. Poikkeamia monitoroidaan ja niihin reagoidaan asianmukaisesti.

Toiminto	Tehtävät lkm v. 2020	Tehtävät lkm v. 2021	Poikkeukset v. 2020	Poikkeukset v. 2021
Eläke– ja työelämäpalvelut	20816	23662	2794	2923
Sijoitustoiminto	944	3287	13	64
Yleisjohto	994	1504	206	210
Rahoituksen ja talouden toiminto	426	187	217	35

3 Kevaan kohdistuvat tietoriskit

Tiedon käsittelyyn kohdistuu aina riskejä, olipa tiedonkäsittely sähköistä tai manuaalista. Kevassa käsitellään paljon dataa ja tietoa, joka on kriittistä sekä Kevan toiminnalle että osittain myös yhteiskunnan ja sosiaaliturvajärjestelmän toimivuudelle. Näin ollen Kevan hallussa olevaan tietoon kohdistuvat riskit on kartoitettava ja niihin on varauduttava huolellisesti.

Kevassa käsiteltävä tieto on suurelta osin asiakkaita koskevaa henkilötietoa, joka on julkisuuslain mukaisesti salassa pidettävää (esimerkiksi terveystietoja). Näihin tietoihin liittyy myös suuria taloudellisia intressejä. Muut salassa pidettävät tiedot perustuvat julkisuuslain sääntelyyn koskien muun muassa liikesalaisuuksia. Myös näiden osalta luottamuksellisuus on erittäin tärkeää ja siihen kohdistuu paljon potentiaalisia riskejä

Kyberriskit ovat läsnä ja voivat realisoitua 24/7

Kevaan kohdistuvien tietoriskien osalta voidaan yleisesti sanoa, että palvelujen digitalisointi ja pilvipalveluihin siirtyminen on johtanut riippuvuuteen

sähköisistä tietojärjestelmistä ja sitä kautta myös tietoturvariskien ja kyberturvariskien korostumiseen. Kevassa jatkettiin vuonna 2021 Pilvipolku-projektia, jonka tarkoituksena on siirtää sovelluspalveluita konesalista pilvipalveluihin. Tässä yhteydessä pilvistrategiassa kartoitettiin myös pilvipalveluihin liittyviä tietoturvariskejä.

Myös muunlaisia riskejä voi ilmetä ja toteutua tietojärjestelmien ja tiedonkäsittelyn kautta ja välityksellä. Ensinnäkin tietotyö ja asiantuntijatyö voi kuormittaa henkilöstöä ja erityisesti uhkaavat tilanteet ja viestit eri kanavissa on tunnistettu riskitekijöiksi. Näiden riskien pienentämiseksi Kevassa tehtiin toimenpiteitä. Kevassa perustettiin uhkatilanneryhmä, joka kartoitti tapahtuneita uhkatilanteita muun muassa kuulemalla esihenkilöitä. Paremman tilannekuvan myötä uhkatilanteen ilmoittamista koskevaa lomaketta muokattiin sujuvammaksi ja uhkatilanneohjetta ja tilanteen käsittelyn prosessia selkeytettiin. Työ jatkuu vuonna 2022 muun muassa henkilöstölle suunnatun uhkatilannekoulutuksen suunnittelulla.

4 Tietosuojan toteutuminen Kevassa

Kevan tietosuojapolitiikka on hyväksytty vuonna 2018 riskienhallinnan johtoryhmässä. Politiikkaan ei ole tehty muutoksia vuoden 2021 aikana. Politiikassa määritellään Kevan tietosuojan tavoitteet, vastuut ja toteutuskeinot. Kevalla on rekisterinpitäjänä vastuu tietojen suojaamisesta. Vastuu jakautuu seuraavasti:

- Organisaation johto (kokonaisvastuu)
- Riskienhallinnan johtoryhmä (hyväksyy, valvoo ja koordinoi)
- Tietosuojavastaava (kehittää, neuvoo ja seuraa tietosuojan toteutumista, yhteistyö)
- Esimiehet (valvovat ja ohjeistavat omia yksiköitään)
- Kevan työntekijät (noudattavat ohjeita ja raportoivat havaitsemistaan ongelmista ja uhkista)

4.1 Kevan henkilötietojen käsittelyperusteet ja rekisteröityjen oikeudet

Tietosuoja-asetus ja muu sääntely koskee henkilötietoja eli kaikkea tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (=rekisteröity) liittyvää tietoa. Henkilötietojen käsittely on myös hyvin laaja käsite, jolla tarkoitetaan eri toimintoja, jotka kohdistetaan henkilötietoihin ja niiden joukkoihin.

Henkilötiedon määritelmä on erittäin laaja

Kevassa henkilötietojen asetuksen mukaiset käsittelyperusteet ovat lakisääteisen tehtävän hoitaminen, sopimus tai rekisteröidyn suostumus. Henkilötietoja on käsiteltävä rekisteröidyn näkökulmasta läpinäkyvästi. Kevan Tietosuoja-sivustolla on saatavissa tätä tarkoitusta varten eri käsittelyperusteisiin ja käyttötarkoituksiin (eläkevakuutetut;

vuokralaiset; työnantajat ja sidosryhmät; työnhakijat; hankinnat; palkkionsaajat) koskevat tietosuojaselosteet. Selosteissa on pyritty kertomaan oleellinen tietosisältö henkilötietojen käsittelystä selkeästi ja teknologianeutraalisti. Näitä selosteita tarkennettiin ja päivitettiin vuoden 2021 aikana.

Rekisteröidyillä on tietosuoja-asetuksen mukainen oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään/ei käsitellä. Jos henkilötietoja käsitellään, rekisteröidyllä on oikeus saada pääsy henkilötietoihinsa sekä oikeus virheellisten tietojen oikaisemiseen tai tietojen poistamiseen. Oikeus poistamiseen ei ole kuitenkaan ehdoton, Kevassa esimerkiksi lakisääteisen tehtävän hoitamiseksi on tarpeen käsitellä vakuutettujen henkilötietoja eikä tietoja voida poistaa. Vuonna 2021 tietosuojavastaavalle tuli 11 kappaletta omien tietojen tarkastuspyyntöjä. Tarkastuspyynnöt voivat olla työläitä, sillä aineistoa voi olla paljon. Samoin voi olla epäselvää, mitä tietoja asiakas todellisuudessa haluaa. Näiden osalta kehitettiin vuonna 2021 pyyntöjä varten oma lomake, jonka avulla asiakas voi helpommin täsmentää tietopyyntöään ja sen perustetta

Kevassa jo työskenteleville laadittua vuonna 2018 henkilötietojen käsittelytoimien taulukkomuotoista kuvausta päivitettiin ja yleiskielistä selostetta täsmennettiin intranettiin.

Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtävänä on neuvoa, kehittää ja valvoa tietosuojalainsäädännön toteutumista Kevassa. Tietosuojavastaava raportoi riskienhallinnan johtoryhmälle. Tietosuojavastaava on myös tiedottanut tietosuojan ajankohtaisista asioista kokouksissa ja vapaamuotoisemmissa yhteistyöryhmissä. Lisäksi tietosuojavastaava on tiedottanut ajankohtaisista asioista Kevan sisäisissä tiedotuskanavissa. Kevan ulkopuolisista ryhmistä tietosuojavastaava on osallistunut Eläketurvakeskuksen tietosuojaryhmän toimintaan. ETK:n tietosuojaryhmässä on pohdittu muun muassa eläkelaitosten ja Kelan yhteistyötä tietojen luovutusten osalta.

Tietosuojavastaava on tarvittaessa osallistunut hankinnoissa henkilötietoja koskevien liitteiden ja ehtojen laatimiseen. Lisäksi tietosuojavastaava on osallistunut lausuntojen laatimiseen lainsäädäntöhankkeista, esimerkiksi hallinnon automaattiseen päätöksentekoon liittyvästä hankkeesta.

Tietosuojavastaava hoitaa myös eläkeasioiden käsittelyn valvontaa. Valvontaa kehitettiin niin, että satunnaisotannalla käsittelyn tietosuojavastaavan valvonta voi kohdistua kaikkiin eläkevakuutettujen tietojen käsittelyyn. Valvonnan uudistus on toiminut ja valvonta on tarkoituksenmukaista.

Tietosuojakoulutusta järjestettiin koulutusta tietosuoja-arvioinnin (DPIA) tekemiseen. Koulutuksen pohjana toimi tietoturva- ja tietosuojakumppanin yhteistyössä kehitetyt työkalut, joiden avulla Kevassa jatkossa tehdään suppeita ja laajoja tietosuojan vaikutustenarviointeja (DPIA, Data Protection Impact Assessment) sekä henkilötietojen siirtojen arviointeja (TIA, Transfer Impact Assessment). Vuonna 2021 tehtiin 11 tietosuojan vaikutustenarviointia. Arviot laadittiin pääosin kokoonpanossa, jossa mukana oli tietosuojavastaavan lisäksi asiantuntija liiketoiminnasta sekä IT-yksiköstä. Vaikutustenarviointeja tullaan tarvittaessa myös päivittämään.

Vuonna 2021 koko henkilökuntaa velvoitettiin suorittamaan verkkokurssi Tietosuojan ABC julkishallinnon henkilöstölle eOppiva-sivustolla.

Koulutusmateriaalin on tuottanut Digi- ja väestötietovirasto, eOppiva, Kuntaliitto ja Oikeusministeriö ja se antaa perustiedot tietosuojasta ja henkilötietojen asianmukaisesta käsittelystä selkeässä, helposti omaksuttavassa muodossa. Tietosuojavastaava vastasi oppimiskokonaisuutta koskeviin kysymyksiin. Yleiset tietosuojaa, tietoturvaa sekä tietohallintoa koskevat ohjeet ovat aina henkilökunnan saatavilla. Uusille työntekijöille on räätälöity perehdyttämismateriaali, joka sisältää myös tietosuojaa käsittelevän osion.

Tietosuojaselosteita päivitettiin ja hankintojen osalta laadittiin uusi tietosuojaseloste Kevan verkkosivuille.

Kevassa on ollut mahdollisuus etätöihin vuodesta 2018 alkaen. 17.3.2020 suurin osa henkilöstöstä siirtyi etätöihin koronapandemian vuoksi. Pääosin etätöissä jatkettiin myös vuonna 2021. Kevan tiloissa tekivät töitä ne, joiden tehtävät edellyttivät fyysistä läsnäoloa. Tietosuojasta etätyössä on ohjeistettu ja kerrottu etätyön kannalta oleelliset seikat henkilötietojen turvallisesta käsittelystä. Mahdollisuuksia etätyön tekemiseen ulkomailla selvitettiin mm. tietosuojan osalta.

4.2 Toimenpide- ja kehittämistarpeet

Henkilötietojen siirrot kolmansiin maihin, erityisesti Yhdysvaltoihin odottaa edelleen EU-tasoista ratkaisua. Asiakkaiden tai henkilökunnan tietoihin ei ole pääsyä EU/ETA-alueen ulkopuolelta Kevan käytössä olevissa palveluissa tai järjestelmissä. Käyttölokien ja metatiedon (siltä osin kuin nämä ovat henkilötietoja) osalta käytäntö riippuu, kuinka järjestelmä on rakennettu. Kevan pilvistrategia osalta on edelleen muistettava tunnistaa kaikki mahdollinen henkilötietojen käsittely, joka tapahtuu EU/ETA:n ulkopuolella, jotta voidaan määritellä oikeanlaiset ja riittävän tehokkaat siirtomekanismit.

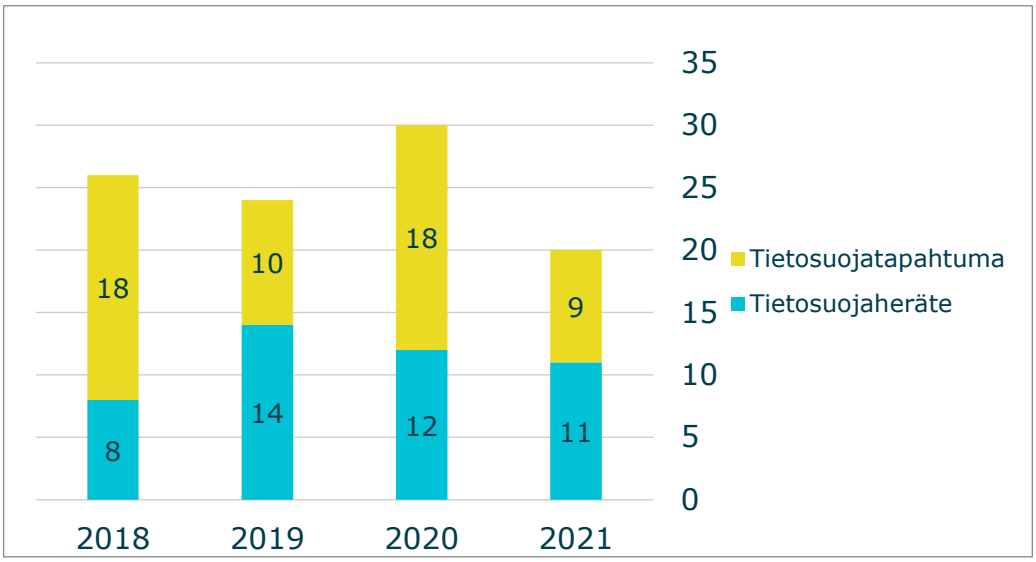
Tietosuojan vuosikello käyttöön

Tietosuojavastaavan vastuualueella on kehittämiskohteena vuodelle 2022 on edelleen osaamisen kehittäminen ja jatkuva oppiminen. Lisäksi tavoitteena on laatia tietosuojan vuosikello, jotta jatkossa vuosittain tehdään tarvittavat toimenpiteet tietosuojatyön parissa. Tarkoituksena on laatia aikataulu, jonka pohjalta on selkeä edetä systemaattisesti muun muassa vaikutustenarviontien päivittämisessä ja henkilökunnan kouluttamisessa.

4.3 Tietosuojatapahtumat ja -herätteet

Yleisen tietosuoja-asetuksen mukaan tietoturvaloukkauksella tarkoitetaan henkilötietoja koskevaa loukkausta, jonka seurauksena käsiteltyjen henkilötietoja on vahingossa tai lainvastaisesti tuhottu, hävitetty, muutettu, luovutettu luvattomasti tai tietoihin päästy asiattomasti. Kevassa tietosuoja-asetuksen mukaiset loukkaukset kirjataan tietosuojatapahtumiksi tai -herätteiksi. Tietosuojavastaava selvittää ja arvioi tilanteen ja tarvittaessa raportoi ylemmälle taholle sekä tekee ilmoituksen tietosuojavaltuutetun toimistoon ja rekisteröidylle. Alla olevassa taulukossa ovat näkyvissä kaikki tietosuojaan liittyvät poikkeamat ja herätteet, oli kyse sitten inhimillisistä tai järjestelmiin

liittyvistä poikkeamista. Tietosuojatapahtuma on tilanne, jossa loukkaus on jollakin asteella tapahtunut. Tietosuojaheräte on signaali, jossa varsinaista loukkausta ei ole tapahtunut. Tapahtumat ja herätteet vuosina 2018-2021 koskivat eläkevakuutettujen tietoja.



1 Tietosuojatapahtumat ja -herätteet vuosina 2018-2021

Vuonna 2021 oli tietosuojatapahtumia, jossa oli kyse inhimillisestä virheestä kuten skannausvirheestä, virheestä asiakaspalvelutilanteessa tai sähköpostiviestinnässä. Osa tapahtumista johtuu yhteistyökumppaneiden virheistä (paperipostin kulku). Kaikki tietosuojatapahtumat on käyty läpi ja on selvitetty esihenkilön kanssa asian kulku. Jos kyse on ollut inhimillisestä virheestä, asiankäsittelijää on ohjeistettu jatkossa kiinnittämään huomiota virheen mahdollisuuksiin. Tietosuojatapahtumat on annettu tiedoksi myös riskienhallinnan johtoryhmälle. Tietosuojavaltuutetulle ilmoitettuja tapahtumia (eli tietoturvaloukkauksia) oli neljä kappaletta vuonna 2021. Tietosuojaherätteiksi kirjataan muun muassa Eläketurvakeskukselta tulevat selvityspyynnöt silloin kun käsitellään ns. VIP-asiakkaita ETK:n rekistereissä. Näiden osalta kaikki käsittelyt ovat liittyneet työtehtäviin.

5 Tietoturvallisuuden toteutuminen Kevassa

Tietoturva on yhtä vahva kuin ketjun heikoin lenkki

Tietoturva on olennainen osa Kevan organisaation riskienhallintaa. Tietoturvallisuudella tarkoitetaan tietojen, palvelujen ja järjestelmien suojaamista niihin kohdistuvien riskien hallitsemiseksi hallinnollisilla ja teknisillä toimenpiteillä. Kevassa on laadittu riskienhallinnan johtoryhmän hyväksymä tietoturvapolitiikka, jossa määritellään Kevan tavoitteet, vastuut ja toimintalinjat koskien tietoturvallisuutta. Tietoturvapolitiikkaa täydentävät käytännöt.

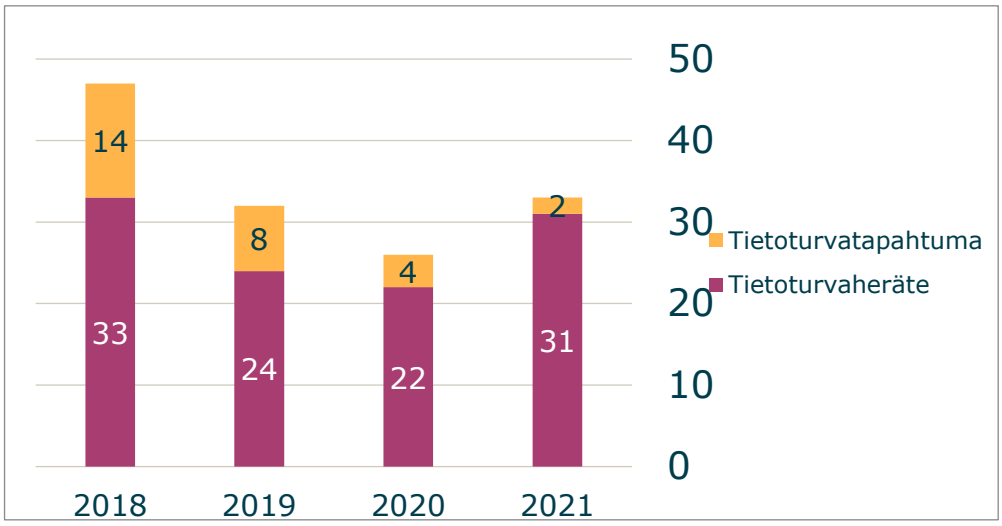
Tietoliikenneturvallisuus kattaa tietojenkäsittely-ympäristön suojauksen, tietoverkkojen rakenteellisen turvallisuuden, suodatussäännöstöt ja langattomien verkkojen turvallisuuden. Tietojärjestelmäturvallisuus kattaa käyttö- ja pääsyoikeuksien hallinnoinnin, tunnistamisen, järjestelmäkovennuksen, haittaohjelmasuojauksen, turvallisuuteen liittyvien tapahtumien jäljitettävyyden, poikkeamahallinnan, salausratkaisut sekä palveluiden ja sovellusten tietoturvavaatimukset. Ohjeiden käytännön toimivuutta ja niiden noudattamista seurataan sekä teknisillä järjestelmillä että auditoinneilla. Henkilöstön ohjeiden osaamistasoa ja palautetta niiden toimivuudesta seurataan laatuauditoinneissa. Jokainen Kevalainen on lisäksi allekirjoittanut salassapitositoumuksen koskien henkilötietoja, joita käsitellään osana työtehtäviä. Fyysinen turvallisuus Kevassa tarkoittaa toimitilojen ja alueiden turvaamista sekä niiden turvallisuusjärjestelmiin ja -laitteisiin liittyviä toimia.

Tietoturva raportoi riskienhallinnan johtoryhmälle ja ohjausryhmänä toimii IT-johtoryhmä, riskienhallintapäälliköllä ja tietosuojavastaavalla täydennettynä. Toimintaa ohjaa ja koordinoi tietoturvapäällikkö, joka saa tukea ja apua IT-johtajalta. Tietoturva palvelee Kevaa tietoturvariskien kartoituksessa, hankinnoissa, eri toimintojen analysoinnissa, tietoturvatestauksessa, haavoittuvuuksien hallinnassa, lokituksen ja käyttövaltuuksien hallinnassa sekä ohjeistuksessa ja kouluttamisessa. Lisäksi tietoturva seuraa havainnoi päivittäin tietoturvan tilaa ja tapahtumia sekä alan yleistä kehitystä.

Vuonna 2021 toteutettiin yhteistyökumppanin kanssa kyberharjoituksen, jossa simuloitiin kuvitteelliset olosuhteet, joissa kyberhäiriön vaikutuksia ja niistä toipumista harjoiteltiin ja testattiin. Tavoitteena oli tunnistaa Kevan toimintaan liittyvistä prosesseista, päätöksenteosta ja viestinnästä heikkoja kohtia sekä korjata niitä. Harjoitusskenaariona käytettiin kuvitteellista laajavaikutteista kyberhyökkäystä Kevan järjestelmiin. Harjoituksen yhteydessä tunnistettiin kehittämiskohteita, ensinnäkin kriisitilanteissa viestinnän sujuvuus on ensiarvoisen tärkeää turvata. Toiseksi harjoittelua on syytä jatkaa, jotta poikkeustilanteessa toimimisesta tulee rutiini, joka sujuu mutkattomasti. Harjoittelua tullaan jatkamaan Kevassa säännöllisesti.

Tietoturvapäällikkö on vuonna 2021 aktiivisesti seurannut ajankohtaisia uutisia sekä tiedottanut ja opastanut kevalaisia onnistuneeseen tietoturvaan. Muun muassa eri organisaatioihin kohdistuneet kyberhyökkäykset sekä laajalle ulottuneet tietojen kalasteluyritykset sekä haittaohjelmat ovat olleet tiedottamisessa esillä.

Tietoturvallisuuden herätteet ovat erilaisia (teknisiä) tapahtumia, jossa poiketaan määritellystä. Ne saattavat olla tahallisesti tai tahattomasti aiheutettuja. Tahallisesti aiheutetuista syntyy tietoturvatapahtuma. Tietoturvatapahtumat raportoidaan riskienhallinnan johtoryhmälle sekä IT-johtoryhmälle. Yllä olevassa taulukossa tietoturvatapahtumat ja -herätteet vuosilta 2018-2021.



2 Tietoturvatapahtumat ja -herätteet 2018-2021

5.1 Lokipolitiikka

Kevan lokipolitiikka on laadittu vuonna 2017 ja se koskee kaikkia Kevan tietojärjestelmiä ja/tai palveluja ylläpitäviä ja käyttäviä henkilöitä. Lokitietoja talletetaan ja käsitellään tietojen, tietoverkkojen ja palvelujen käytön ja toiminnan tapahtumien dokumentoimiseksi, sekä häiriö- ja väärinkäyttötilanteiden estämiseksi, havaitsemiseksi ja selvittämiseksi. Lisäksi lokitietoja voidaan käyttää tietoverkkojen ja palvelujen teknistä kehittämistä varten. Lokitiedot ovat myös tarpeen tietosuojan varmistamiseksi. Lokipolitiikkaa päivitettiin vuonna 2021 lokitietojen säilyttämisen osalta.

On huomattava, että lokitiedot eivät ole varsinaisesti Kevan asiakkaan henkilötietoja, vaan Kevan henkilökunnan henkilötietoja ja ne ovat myös julkisuuslaissa mainittuja salassa pidettäviä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevia ja niiden toteuttamiseen vaikuttavia tietoja. Näin ollen lähtökohta on, että asiakkaille luovutetaan lokidataa vain, mikäli asiakkaalle muodostuu julkisuuslain mukainen asianosaisasema ja on perusteltu syy epäillä väärinkäytöksiä. Lokitietojen jälkikäteinen tarkastaminen voi olla tällaisessa tilanteessa tarpeen ja näin ollen keskitetyn lokihallinnan onkin mahdollistettava lokitietodata, joka on riittävän selkeää ja käyttäjäystävällistä, jotta se palvelisi tarkoitustaan. Vuonna 2021 vastattiin kahteen lokitietopyyntöön.

6 Lopuksi

Vastuullinen tiedonhallinta, tietoturvallisuus ja tietosuojavaatimusten huomioonottaminen palvelevat Kevan perustehtävää eli eläketurvan toimeenpanoa sekä Kevan muita toimintaperiaatteita sekä strategiaa. Tietoturvan ja tietosuojan varmistaminen korostuu entisestään ottaen huomioon maailmanpolitiikan kehityksen. Varautumista esimerkiksi tietoliikennehäiriöihin ja kyberhäirintään on tehty Kevassa jo aiemmin, mutta työ jatkuu intensiivisesti vuonna 2022.