Tietotilinpäätös 2020

Sisällysluettelo

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, 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 on laadittu tietotilinpäätös viimeksi vuodelta 2016, jolloin ennakoitiin voimaan tulevaa yleistä tietosuoja-asetusta ja sitä täsmentävää kansallista lainsäädäntöä. Tuossa tietotilinpäätöksessä keskityttiin ainoastaan vakuutettuja koskevien henkilötietojen käsittelyyn. Raportissa tunnistettiin kaikki Kevan tarjoamat palvelut ja rekisterit, joissa käsitellään vakuutettujen henkilötietoja sekä arvioitiin niiden asianmukaisuutta sekä kehittämiskohteita. Tuolloin todettiin, että kokonaisuudessaan tietosuojan asema organisaation keskeisenä osa-alueena on tunnistettu ja tietosuojavastaavan roolia on terävöitetty etenkin etu-painotteisena sisäisenä neuvonantajana kaikille toiminnan osa-alueille.

Vuoden 2020 tietotilinpäätös jakautuu Kevaa koskeviin tietoriskeihin, tiedonhallintaa, tietoturvaa sekä tietosuojaa käsitteleviin lukuihin. Tämä jaottelu on tarkoituksenmukainen, sillä henkilötietojen käsittely ei tapahdu tyhjiössä vaan siihen liittyvät oleellisesti tietoturvakysymykset eli muun muassa tekniset suojauskeinot. Tämän lisäksi tiedonhallinta ja sen järjestelyt ovat käytännössä tieto-organisaation selkäranka. Lisäksi tällä jaottelulla on helppo havainnollistaa eri osa-alueiden eroja, arkipuheessa tietosuoja ja tietoturva usein samaksi asiaksi, mitä ne siis eivät ole. Kevassa henkilötietojen suojaa koskevan lainsäädännön lisäksi on otettava huomioon paljon muuta tietoa koskevaa sääntelyä ja näiden yhteensovittaminen on ajoittain haasteellista.

Tietotilinpäätöksen laatiminen ei onnistuisi tietosuojavastaavalta yksin, joten suuri kiitos kaikille, jotka ovat antaneet tietoja ja avustaneet selvitystyössä.

2 Yleiskatsaus ja tilannearvio

2.1 Tietosuojan tilanne

Yleisesti ottaen Kevassa tietosuoja-asiat huomioidaan hyvin ja niihin suhtaudutaan vakavasti. Eri yksiköissä mahdollisia tietosuojapuutteita tunnistetaan ja niihin myös puututaan. Tietosuojavastaavan ja yksiköiden välinen yhteistyö on sujunut hyvin ja kynnys konsultoida tietosuojavastaavaa on matala. Lisäksi tietosuojaongelmiin on reagoitu nopeasti ja tehty tarkoituksenmukaiset toimenpiteet.

Tietosuojan osalta kehityskohteitakin on noussut esiin. Hankintaprosessin ja sopimusten valmistelun sekä uusien palvelujen käyttöönoton osalta yhteistyö ja koordinointi olisi aloitettava jo aiemmassa vaiheessa, jotta voitaisiin varmistaa Kevan intressien toteutuminen ja jotta muistettaisiin ottaa huomioon kaikki henkilötietojen käsittelyn kannalta merkitykselliset seikat jo etukäteen. Tietoturvan ja tietosuojan osalta sopimusliitteitä olisi tarpeen edelleen kehittää. Kevan solmimissa sopimuksissa on varmistettu, että ulkopuoliset henkilötietojen käsittelijät ilmoittavat mahdollisista tietoturvaloukkauksista Kevalle. Sopimushallinnan keinoin on kuitenkin jatkuvasti kehitettävä sopimusten valvontaa myös siitä näkökulmasta, että mahdolliset loukkaukset tosiasiallisesti tulevat Kevan tietoon.

Ohjeistusta tietosuoja-asioihin liittyen on mahdollisesti ollut vaikea löytää henkilöstölle suunnatuista kanavista. Tältä osin viestintä on otettava jatkossa mukaan aikaisessa vaiheessa, kun uusia ohjeita laaditaan. Eläkekäsittelynvalvonta on myös noussut esiin kehityskohteena.

Kevassa aloitettiin vuonna 2020 Pilvipolku -strategian valmistelu alkukartoituksella, joka valmistui maaliskuussa 2021. Tarkoituksena on luopua oman konesalin ylläpidosta ja siirtyä käyttämään pääsääntöisesti pilvipalveluita. Oman konesalin rakentaminen ja ylläpito aiheuttavat kustannuksia, joita voidaan pienentää ulkoistamalla palvelut pilveen. Tällöin resursseja voidaan kohdistaa oman liiketoiminnan ytimeen. Pilvipalveluihin siirtyminen aiheuttaa myös haasteita tietosuojan ja tietoturvan näkökulmasta, jotka on huomioitava pilvistrategian laatimisessa.

2.2 Tietoturvan tilanne

Kevan tietoturvaan on panostettu merkittävästi viimeisten vuosien aikana. Vuonna 2020 yhtenäistimme tietoturvan havainnointi- ja valvontavälineistöä paremmin tukemaan kokonaistilannekuvaa tietoturvasta. Tietoturvaa seurataan jatkuvasti Kevan tietoturvakumppanin ja Kevan itsensä toimesta. Kohdistettuja hyökkäyksiä Kevaan tehdään lähes päivittäin, mutta toistaiseksi yritykset eivät ole tuottaneet tulosta, vaan Kevan tietoturvapuolustus on joko havainnut tai estänyt ne.

Keva on jatkanut henkilöstön kouluttamista sähköpostin kautta tulleiden haittaohjelmien havaitsemiseksi. Käyttäjille lähetetään simuloituja viestejä, jotka mahdollisuuksien mukaan pyrkivät olemaan hyvin samankaltaisia kuin oikeatkin huijausviestit. Jos viestiin haksahtaa eli avaa viestissä olevan linkin, käyttäjä ohjautuu koulutussivustolle, jossa käydään ne asiat läpi joiden perusteella viesti olisi pitänyt tunnistaa huijaukseksi. Kevassa pidetään myös säännöllisiä harjoituksia tietoturvatapahtumiin liittyen.

Kevan sähköpostiin on määritelty myös vinkki, joka kertoo, jos viestiä ollaan lähettämässä Kevan ulkopuolelle. Tällä pyritään ehkäisemään vahingossa tapahtuva tietojen vuoto. Työeläketoimijoiden kesken on suunnitteilla otettavaksi käyttöön sähköpostien vahvempi suojaus, jossa itse siirtoväylän suojauksen lisäksi itse viesti suojattaisiin siten, että ulkopuoliset eivät siihen pääsisi käsiksi.

Toimittajien ja Kevan välisiin sopimuksiin on otettu käyttöön erillinen tietoturvasopimus, johon on koottu tärkeimmät tietoturvaan liittyvät toimenpiteet, joita edellytämme toimittajiltamme. Tietosuoja- ja tietoturvasopimusliitteet on katsottu yhdessä tietosuojavastaavan kanssa läpi niin, että ne kattaisivat mahdollisimman hyvin hankittavan kokonaisuuden.

Tietoturvaa kehitetään myös jatkuvasti. Keva on tehnyt itsearvioinnin Traficomin julkaisemalla kybermittari-työkalulla ja saanut siitä erittäin hyviä kehittämiskohteita. Tietoturvan ulkoisten sidosryhmien kanssa tehdään jatkuvaa yhteistyötä. Lisäksi olemme kilpailuttaneet tietoturvan valvontakumppanimme, jolle Kevan tietoturvan valvonta siirtyy vuoden 2021 loppuun mennessä. Pilvipalveluiden laajentuvan käytön suunnittelussa tietoturvalla on keskeinen rooli. Pilvipalvelut voidaan ottaa käyttöön tietoturvallisesti vaarantamatta tietosuojaa.

2.3 Tiedonhallinnan tilanne

Tiedonhallinnan osalta vuosina 2019 ja 2020 työtä aiheuttivat lainsäädäntömuutokset. Julkisen hallinnon tiedonhallinnasta annettu laki (906/2019) tuli voimaan 1.1.2020 siirtymäaikoineen ja Kevassa siirtymää valmisteli valmistautumistyöryhmä vuodesta 2019 alkaen.

Lain tavoitteena on toteuttaa hyvää hallintoa ja julkisuusperiaatetta. Lisäksi sen tarkoituksena on edistää julkishallinnon tietovarantojen digitalisoitumista ja digiturvallisuutta, yhteentoimivuutta, tiedon jakamista ja hyödyntämistä. Kyseessä on yleislaki ja sen soveltamisala on laaja. On hyvä huomata, että tiedonhallintalain velvoitteiden täyttäminen ei kosketa pelkästään perinteisen asiakirjahallinnon ammattilaisia vaan se työllistää eri ammattiryhmiä kuten organisaation johtoa, tietoturva-asiantuntijoita, it-asiantuntijoita, riskienhallintaa, tietosuojavastaavaa ja henkilöstöhallintoa. Lainsäädännön mukaiset vaatimukset saatiin täytettyä hyvin, tiedonohjaussuunnitelmaan vaadittavat käsittelyvaiheet viimeistellään vuoden 2021 aikana.

Kehityskohteena jatkossa tiedonhallinnan osalta voidaan mainita ainakin tiedolla johtamisen prosessit. Tiedolla johtaminen tarkoittaa oikeaan tietoon perustuvaa päätöksentekoa, jossa oikea tieto saadaan dataa analysoimalla, mikä on myös Kevan tavoitteena. Dataa ja tietoa käsitellään Kevassa todella paljon, mutta data on jalostettava sopivaan muotoon ja johtamista tukeviksi prosesseiksi. Riskienhallinnan näkökulmasta kokonaisvaltainen työkalu eli GRC-tietojärjestelmä mahdollistaisi toiminnan laadun ja tehokkuuden parantamisen sekä paremman tilannekuvan tiedolla johtamisen tueksi.

3 Tiedonhallinta Kevassa

Vuoden 2020 alussa tuli voimaan julkisen hallinnon tiedonhallinnasta annettu laki (906/2019), mikä myös asetti Kevalle tietohallintoon liittyviä muutostarpeita. Keva noudattaa lisäksi toiminnassaan ja tiedonhallinnassaan viranomaisen toiminnan julkisuudesta annettua lakia (621/1999), arkistolakia (831/1994), EU:n yleistä tietosuoja-asetusta (2016/679), tietosuojalakia (1050/2018), potilaan asemasta ja oikeuksista annettua lakia (785/1992) sekä asetusta viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999).

Kevan tietohallinnon pääperiaatteet ja toimintatavat on dokumentoitu Tiedonhallintapolitiikka-asiakirjaan, joka on hyväksytty johtoryhmässä vuonna 2020. 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 toteutetaan Kevan sisäisenä yhteistyönä.

Tiedonhallintamallilla täytetään tiedonhallintalain velvoitteita Kevan osalta. Vuosien 2019 ja 2020 aikana täydennettiin tiedonhallintalain vaatimat kuvaukset, pohjina käytettiin seuraavia olemassa olevia kuvauksia: Toimintaprosesseista, Tietovarannoista ja tietoaineistojen arkistoinnista, Tietojärjestelmistä ja Tietoturvallisuus toimenpiteistä. Tiedonhallintamalli muodostuu näiden kuvausten kokonaisuudesta.

Julkisen hallinnon tiedonhallinnasta annetun lain mukaan tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on ajantasaiset ohjeet tiedonhallinnan vastuiden toteuttamisesta. Kevassa on toimitusjohtajan päätös tiedonhallinnan vastuista. Tarkemmin vastuita konkreettisten tehtävien kautta on kuvattu ohjeessa Tiedonhallinnan vastuiden toteuttaminen Kevassa, jonka johtoryhmä on hyväksynyt.

ICT-johtaja vastaa tiedonhallintamallin ylläpidosta ja hyväksyy tiedonhallintamallin päivitykset, tekniset korjaukset ja vähäiset muutokset. Mikäli tiedonhallintamalliin tehdään merkittäviä muutoksia, muutokset hyväksyy toimitusjohtaja. Hyväksymisen jälkeen merkittäviä muutoksia tiedonhallintamalliin ei ole tullut.

Tiedonhallintayksikön on julkisuusperiaatteen toteuttamista varten ylläpidettävä kuvausta sen hallinnoimista tietovarannoista ja asiarekisteristä. Kuvauksella tuetaan hyvää tiedonhallintatapaa ja läpinäkyvää hallintoa. Lisäksi varmistetaan tiedonsaantioikeuksien toteutuminen Kevassa. Kuvauksen julkista osaa ylläpidetään Kevan verkkosivuilla.

Asiakirjahallinnossa otettiin vuonna 2020 robotti tuotantokäyttöön. Yleisesti ottaen robotiikkaa käytettiin eniten eläke- ja työelämäpalveluissa, joissa tehtäviä oli yli 20 000 kappaletta. Rahoituksen ja talouden toiminnossa robotti suoritti tehtäviä n. 400 kpl sijoitustoiminnossa ja yleisjohdossa molemmissa n. 900 kappaletta.

3.1 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. Alla yleiskuva siitä, minkälaista tietoa Kevassa käsitellään.

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)

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.

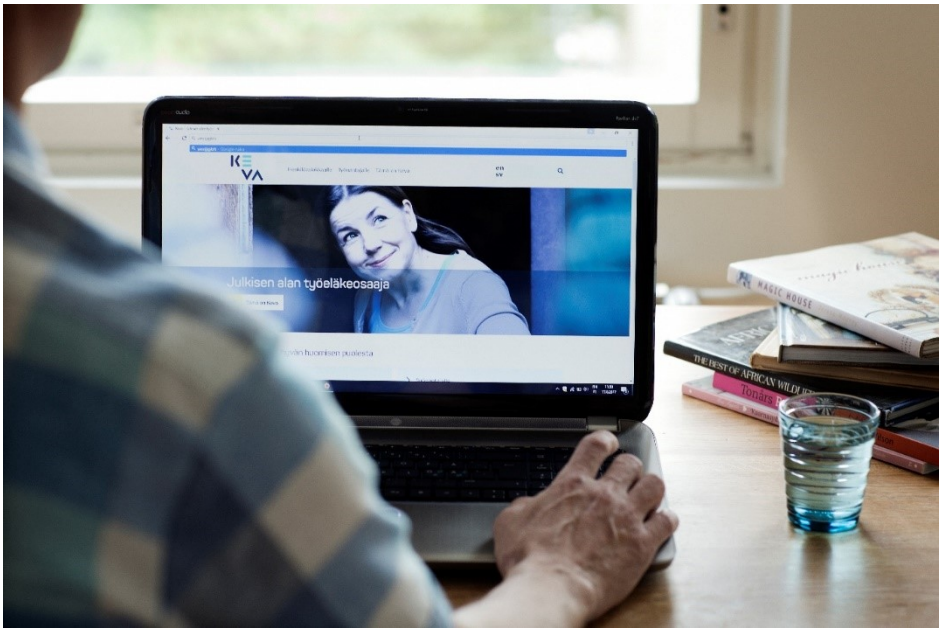
- Liikesalaisuudet (Kevan ja sopimuskumppanien)
- Turvajärjestelyt
- Poikkeusoloihin varautuminen
- Oikeudenkäynnin osapuolena oikeudenkäyntiin valmistautumista koskevat tiedot

3.2 Julkisuusperiaatteen toteutuminen

Pääsääntöisesti kaikki Kevan asiakirjat ovat 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. Näin ollen julkisuuslain soveltamisala ja luovutusperusteet eivät ole aina täysin selkeitä ja ne ovat herättäneet kysymyksiä. Julkisuuslain soveltaminen voi olla haasteellista, sillä tietojen luovuttamista säädellään myös muualla kuin julkisuuslaissa.

Tietosuojavastaava otti kantaa julkisuuslain alaisiin tietopyyntöihin liittyen työntekijän valintaprosessiin sisältyvien tietojen julkisuudesta sekä vanhojen eläkeasiakirjojen luovutuksen reunaehdoista. Samoin on otettu kantaa, minkälainen velvollisuus Kevalla on tuottaa aineistoa tietopyyntöihin vastaamisen yhteydessä.

Kevalaisia on ohjeistettu julkisuusperiaatteen toteuttamiseen ja neuvoja on voinut tarvittaessa pyytää juridisista palveluista.



Vuonna 2020 julkisuuslain perusteella tehtyjä tietopyyntöjä oli 29 kappaletta. Useimmin toistuva pyyntö koskee kansanedustajien sopeutumisrahan saajia, joita tiedustelevat eri tiedotusvälineiden edustajat.

4 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

Palvelujen digitalisointi johtaa kyberturvariskien korostumiseen

Kevaan kohdistuvien tietoriskien osalta voidaan yleisesti sanoa, että palvelujen digitalisointi on johtanut riippuvuuteen sähköisistä tietojärjestelmistä ja sitä kautta myös tietoturvariskien ja kyberturvariskien korostumiseen. Suunnitellusta pilvipalveluihin siirtymisestä johtuu, että erilaisia ja mahdollisesti uusia tietoriskejä esiintyy ja niihin on jatkossakin kiinnitettävä tarkasti huomiota. Tietoturvan tekniset kysymykset eivät kuitenkaan ole ainoita merkittäviä tietoon kohdistuva riskejä.

Tietoon kohdistuvat riskit ja loukkaukset voivat ilmetä:

- tiedon saatavuudessa eli tietoon ei päästä
- tiedon eheydessä eli tietoa päästään muuttamaan tai poistamaan tai se on virheellistä
- tiedon luottamuksellisuudessa eli tietoa vuotaa

Tietoon kohdistuvien riskien arvioinnissa ja niihin varautumisessa huomioidaan seuraavia seikkoja:

- Johtaminen
  - Suunnitelmat ja strategiat poikkeustilanteita varten
- Lainsäädäntö ja muut sääntelylähteet
  - Yleis- ja erityislait, joita sovelletaan Kevaan
  - Korvausvelvollisuus
- Tietojärjestelmät ja tekninen tietoturva
  - Haittaohjelmat, tietomurrot, palvelunestohyökkäykset
  - Datan vapaa liikkuvuus pilvipalveluissa
  - Pääsynhallinta ja -valvonta
  - Tietojärjestelmien sinänsä virheettömät ominaisuudet sekä virheet
  - Järjestelmien ylläpito
- Henkilöstö
  - Osaaminen, kouluttaminen, toimintatavat

  - Etätyö
  - Henkilöstön valvonta
  - Rekrytointi
- Sopimukset ja tietosuoja
  - Hankintaprosessin ja tarjouspyynnön valmistelu
  - Sopimusehdot (esim. henkilötietojen käsittelyn ehdot, exit-ehdot)
- Fyysinen turvallisuus
  - Kulunvalvonta ja vartiointi
- Viestintä ja tiedottaminen
- Seuraukset ulkopuolisille, esimerkiksi yhteiskunnalle

Tietoriskien realisoituminen voi aiheuttaa Kevalla myös mainehaittoja ja/tai korvausvelvollisuuksia. Tietoriskiksi voidaan laskea tapahtuma vuoden 2020 joulukuussa, kun inhimillisestä virheestä johtui, että tammikuun 2021 eläkkeet maksettiin kunta-alan eläkeasiakkaiden tileille jo joulukuussa. Maksuvirhe saatiin korjattua siltä osin, ettei asiakkaille koitunut haitallisia veroseuraamuksia eikä tilanne vaatinut asiakkailta toimenpiteitä. Virheestä tiedotettiin ja asiasta uutisoitiin valtakunnallisissa medioissa. Lisäksi oikeusasiamiehelle tehtiin asiasta kanteluita, jotka ratkaistiin vuonna 2021. Apulaisoikeusasiamies totesi ratkaisussaan EOAK/8285/2020, että Keva oli toiminut tilanteessa asianmukaisesti ja eläkkeensaajien etujen mukaisesti. Virheen johdosta päätettiin muuttaa maksuprosessia niin, ettei samankaltaisia virheitä voi sattua jatkossa.

Turvataan tiedon luottamuksellisuus, eheys ja saavutettavuus

5 Tietosuojan toteutuminen Kevassa

Kevan tietosuojapolitiikka on hyväksytty vuonna 2018 riskienhallinnan johtoryhmässä. 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)

5.1 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.

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) koskevat tietosuojaselosteet. Selosteissa on pyritty kertomaan oleellinen tietosisältö henkilötietojen käsittelystä selkeästi ja teknologianeutraalisti. Näihin on tarpeen tehdä pieniä tarkennuksia.

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 2020 tietosuojavastaavan tietoon tuli 14 kappaletta omien tietojen tarkastuspyyntöjä. Tarkastuspyynnöt voivat olla työläitä, sillä aineistoa voi olla paljon. Samoin voi olla epäselvää, mitä tietoja asiakas todellisuudessa haluaa. Näiden osalta kehittämiskohteina nousivat esiin vuodelle 2021 selkeä ja yksilöity pyyntölomake sekä selkeä työnjako, silloin kun pyynnöt koskevat lääketieteellisiä asiakirjoja.

Kevassa jo työskenteleville on laadittu vuonna 2018 henkilötietojen käsittelytoimien taulukkomuotoinen kuvaus Tukevassa, joka tulee päivittää vuoden 2021 aikana. Samoin yleiskielinen tietosuojaseloste koskien työntekijöitä olisi laadittava.

5.2 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. Kevan ulkopuolisista ryhmistä tietosuojavastaava on osallistunut Eläketurvakeskuksen tietosuojaryhmän toimintaan sekä osallistuminen Vahtityöryhmään Tietosuojan kehittäminen. ETK:n ryhmässä on pohdittu muun muassa tietojen säilytysaikoihin liittyviä säännöksiä.

Tietosuojavastaava on tarvittaessa osallistunut hankinnoissa henkilötietoja koskevien liitteiden ja ehtojen laatimiseen. Lisäksi tietosuojavastaava on osallistunut lausuntojen laatimiseen lainsäädäntöhankkeista, esimerkiksi arviomuistiosta hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista.

Tietosuojavastaava hoitaa myös eläkeasioiden käsittelyn valvontaa. Valvontaa kohdistetaan korostetusti tiettyihin henkilötietoryhmiin, millä varmistetaan, ettei henkilöiden tietoja avata ja tarkastella turhaan. Valvonnan kehittämistarpeet ovat nousseet esiin ja valvontaa ollaan kehittämässä niin, että valvonnasta tulisi normaali ja rutiininomainen osa eläkeasian käsittelyn prosesseja.

Tietosuojakoulutusta on järjestetty liiketoiminnan tiimeille vuonna 2020. Uutena asiana on käsitelty asiakkaan ja viranomaisen puhelintunnistusta. Ohjeet koskevat kaikkea puhelinasiointia, joissa on tarpeen tunnistaa henkilö. Lisäksi puhelintallenteisiin liittyen on laadittu ohjeet. Linkkien käytöstä Kevasta lähetettävissä erilaisissa viesteissä on tehty ohjeistus. Lisäksi ulkopuolelle lähteviin sähköposteihin on lisätty huomioteksti, jottei lähetettäisi vahingossa salassa pidettävää tietoa väärälle vastaanottajalle. Yleiset tietosuojaa, tietoturvaa sekä tietohallintoa koskevat ohjeet ovat aina henkilökunnan saatavilla.

Henkilötietojen tietoturvaloukkaus on tietosuoja-asetuksen mukaan siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Tietoturvaloukkauksesta on ohjeistettu kirjallisesti ja koulutuksissa asiaa on nostettu esiin. Tiedon joutuminen väärän tahon käsiin on yleisin tilanne. Koulutusten myötä Kevan henkilökunta on tullut yhä tietoisemmaksi ylipäätään tietosuojasta ja tietosuojavastaavalta kysytään etukäteen, miten tulee toimia.

Uusille työntekijöille on räätälöity perehdyttämismateriaali, joka sisältää myös tietosuojaa käsittelevän osion. Yleistä tietosuojakoulutusta ollaan lisäämässä syksyllä 2021 (Tietosuojan ABC).

Asiakkaille suunnattua ohjeistusta ja tulkintoja liittyen työnantajille annettaviin tietoihin on tehty ja kehitetty paljon. Kirjeitse menevien tietojen näyttäminen on siirretty työnantajan verkkopalveluun, mikä osaltaan edistää tietosuojaa. Chatbot-palvelua on kehitetty niin että botti neuvoo myös kirjautunutta asiakasta ja nämä keskustelut jäävät talteen asiakkaan tietoihin. Lisäksi verkkosivujen evästeitä koskevaa informointia on kehitetty.

Kevassa on ollut mahdollisuus etätöihin vuodesta 2018 alkaen. 17.3.2020 suurin osa henkilöstöstä siirtyi etätöihin koronapandemian vuoksi. Kevan tiloissa tekivät töitä ne, joiden tehtävät edellyttivät fyysistä läsnäoloa. Tietosuojasta etätyössä on ohjeistettu ja kerrottu etätyön kannalta oleelliset seikat henkilötietojen turvallisesta käsittelystä. Jatkossakin etätyömahdollisuuksien mahdollisesti laajentuessa on pidettävä ohjeistusta ajan tasalla ja viestittävä asiasta.

5.3 Toimenpide- ja kehittämistarpeet

Tietosuojan osalta huomioita ja toimenpidetarpeita on noussut EU-lainsäädännön ja siihen liittyvän oikeuskäytännön perusteella. Brexitin siirtymäaika tietosuojan osalta loppui 30.6.2021. Tätä ennen komissio hyväksyi määräaikaisen päätöksen tietosuojan tason riittävyydestä Yhdistyneessä kuningaskunnassa. Kevassa käsitellään sosiaaliturva-asetuksen sekä erosopimuksen perusteella eläkeasioiden hoitamisen yhteydessä henkilötietoja, joita myös siirretään eläketurvan hoitamiseksi henkilötietoja Isoon-Britanniaan sähköisen tietojenvaihtojärjestelmä EESSIn kautta. Tältä osin tietojen siirto voi komission päätöksen voimassaoloaikana jatkua kuten ennenkin. Tällä hetkellä Kevassa ei ole muita tilanteita esimerkiksi hankintasopimusten osalta, joissa tapahtuisi henkilötietojen käsittelyä Isossa-Britanniassa.

Kesäkuussa 2020 annettiin Euroopan unionin tuomioistuimessa (EUT) tietosuojaa koskeva tuomio C-311/18 Schrems II, joka koskee siirtomekanismi Privacy Shieldiä ja tietojen siirtoa Yhdysvaltoihin. Tuomioistuin totesi Privacy Shield -järjestelyn tietosuojan tason riittämättömäksi, mikä on aiheuttanut ja aiheuttaa jatkossa kysymyksiä, millä tavalla henkilötietoja voidaan käsitellä Yhdysvalloissa lainmukaisesti. Euroopan tietosuojaneuvosto eli EDBP on laatinut ohjeita siirtoihin, mutta jokainen tapaus on tarkasteltava erikseen.

Olemassa olevien sopimusten ja järjestelmien osalta henkilötietojen käsittelyn suhteen Kevassa on edellytetty pääsääntöisesti käsittelyä ainoastaan EU/ETA-alueella. Sijoitustoimintojen osalta tuomion ja rahanpesulainsäädännön vaatimuksien yhteensovittamisesta todettiin, että KYC-tarkoitus (know your customer) voi vaatia henkilötietojen siirtämistä EU/ETA-alueen ulkopuolelle. Siirtoperusteita ovat olleet vakiosopimuslausekkeet, yritystä koskevat sitovat säännöt, nyt kumottu Privacy Shield sekä tietosuoja-asetuksen poikkeus eli 49 artikla.

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 pilvistrategian kannalta on jatkossakin oleellista tunnistaa kaikki henkilötietojen käsittely, joka tapahtuu EU/ETA:n ulkopuolella, jotta voidaan määritellä oikeanlaiset ja riittävän tehokkaat siirtomekanismit. EU-tasoista ratkaisua voidaan odottaa Yhdysvaltoihin siirtojen osalta, mutta aikataulu on avoin.

Tietosuojan vaikutustenarvioinnin tekeminen tutuksi vuoden 2021 aikana

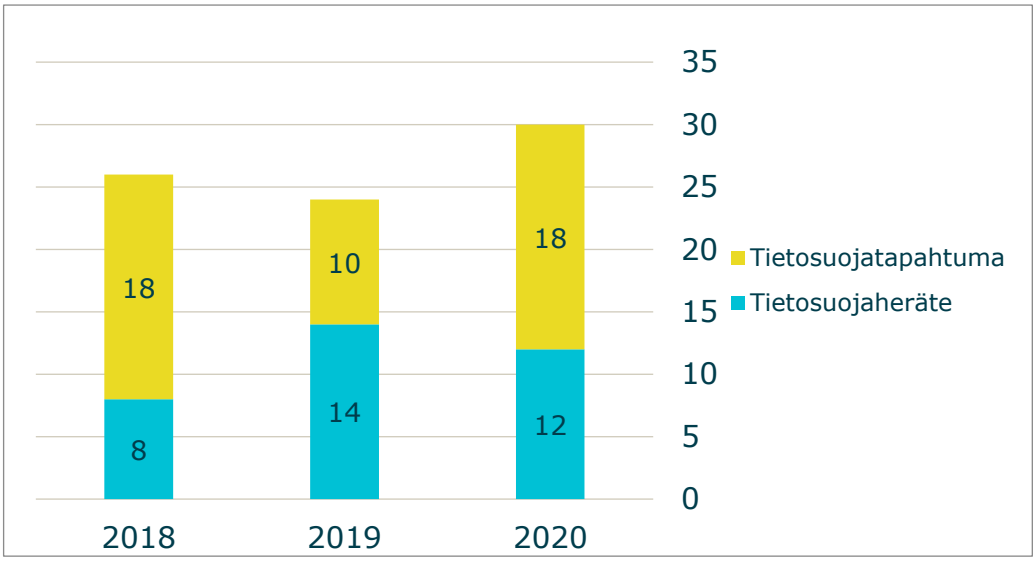
Kevassa on vuonna 2020 kehitetty tietoturva- ja tietosuojakumppanin kanssa tietosuojan vaikutustenarviointia. Työ jatkuu vuonna 2021. Tavoitteena on, että tietosuojan vaikutustenarviointeja (DPIA) tehdään ja pidetään yllä säännöllisesti yhdessä tuoteomistajien ja IT-vastuuhenkilöiden kanssa. Lisäksi TIA-arviointeja (Transfer Impact Assessment) tullaan tekemään muun muassa pilvipalveluiden osalta silloin kun tietoja siirretään EU/ETA-alueen ulkopuolelle. DPIA:n tekemisestä tullaan jatkossa kouluttamaan esimerkiksi tiimien esihenkilöitä.

Hankintojen yhteydessä kerätään palveluntuottajien yhteystietoja sekä heidän alaistensa henkilötietoja muun muassa silloin, kun palveluntuottajan henkilökunnalta vaaditaan nimetty asiantuntija, jolla on riittävä koulutus ja työkokemus palvelun tuottamiseen. Tältä osin hankintojen kilpailutuksiin osallistuvia henkilöitä koskeva tietosuojaseloste tulisi myös laatia.

5.4 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 2018-2020 koskivat eläkevakuutettujen tietoja.



1 Tietosuojatapahtumat ja -herätteet vuosina 2018-2020

Vuonna 2020 oli useampi tietosuojatapahtuma, jossa oli kyse inhimillisestä virheestä. Yleensä ottaen kaikki tietosuojatapahtumat on käyty läpi ja on selvitetty esimiehen kanssa asian kulku. Jos kyse on ollut inhimillisestä virheestä, esimies on käsitellyt tapauksen ko. käsittelijän kanssa ja painottanut tarkkuutta henkilötietojen käsittelyssä ja tarvittaessa ohjeistanut lisää. Tietosuojatapahtumat on annettu tiedoksi myös riskienhallinnan johtoryhmälle.

6 Tietoturvallisuuden toteutuminen Kevassa

Tietoturva kuuluu kaikille Kevalaisille!

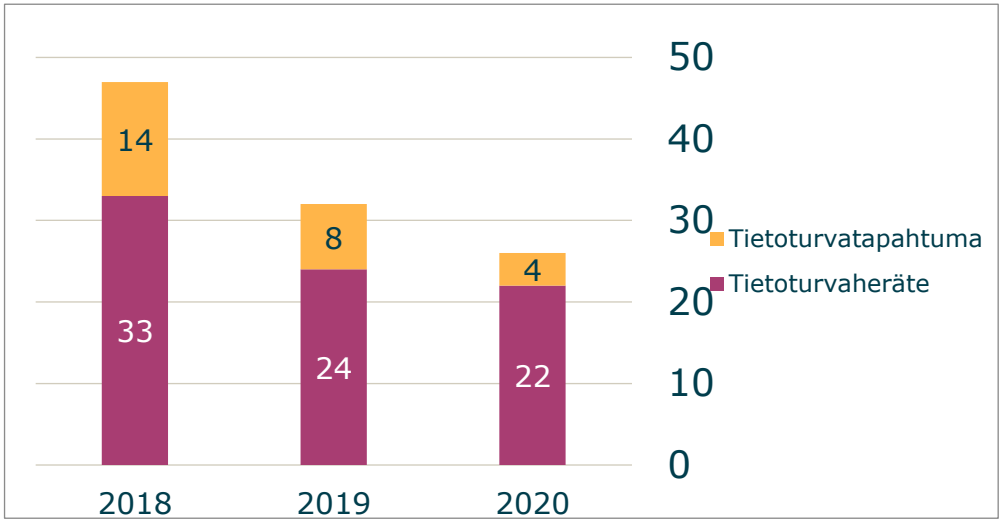
Keva huolehtii korkeasta tietoturvan tasosta järjestelmissään. Tietoturvallisuudella tarkoitetaan tietojen, palvelujen ja järjestelmien suojaamista niihin kohdistuvien riskien hallitsemiseksi hallinnollisilla ja teknisillä toimenpiteillä. Kevassa on laadittu riskien hallinnan johtoryhmän hyväksymä tietoturvapolitiikka, jossa määritellään Kevan tavoitteet, vastuut ja toimintalinjat koskien tietoturvallisuutta. Tietoturvapolitiikkaa täydentävät käytännöt. Tietoturvallisuudesta huolehtiminen kuuluu kaikille Kevalaisille, johtoryhmästä loppukäyttäjään, oman roolinsa mukaisesti.

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.

Koronavuonna ei järjestetty henkilökunnan koulutustilaisuuksia tietoturvaan liittyen, mutta tietoturva-asioista viestittiin henkilökunnalle aktiivisesti eri viestintäkanavissa.

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. Alla olevassa taulukossa tietoturvatapahtumat ja -herätteet vuosilta 2018-2020.



2 Tietoturvatapahtumat ja -herätteet 2018-2020

6.1 Lokipolitiikka

Kevan lokipolitiikka 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.

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.

7 Lopuksi

Yhteenvetona voidaan todeta, että Kevassa on ymmärretty hyvin tiedon ja datan arvo sekä niiden liikkuvuuteen ja käsittelyyn liittyvät riskit. Tietoriskien hallinta ja mitigointi vaativat jatkuvaa seurantaa. Vastuullinen tiedonhallinta, tietoturvallisuus ja tietosuojavaatimusten huomioonottaminen palvelevat Kevan perustehtävää eli eläketurvan toimeenpanoa sekä Kevan muita toimintaperiaatteita sekä strategiaa. Kehitystyö tiedonhallinnan ja tietojen käsittelyn parissa jatkuu, toimintaperiaatteiden ja strategisten tavoitteiden viitoittamana.