Tietotilinpäätös 2022

Heidi Hernetkoski, tietosuojavastaava

Sisällysluettelo

1 Johdanto

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.

Kevassa käsitellään toiminnan luonteen vuoksi paljon vakuutettujen ja muiden asiakkaiden henkilötietoja, joten vastuullisuus ja läpinäkyvyys henkilötietojen käsittelyssä korostuvat. Tässä tietotilinpäätöksessä kerrotaan tiedonhallinnan, tietoturvan sekä tietosuojan toiminnasta vuonna 2022. Tilinpäätöksessä avataan lukujen ja käytännön esimerkkien avulla, kuinka jatkuva työ on sujunut ja mitkä ovat Kevassa kehityskohteita vuonna 2023.

2 Yleiskatsaus

Vuoden 2022 alkupuolella Euroopassa alkanut sotatilanne vaikutti myös Kevan toimintaan. Riskienhallinnan näkökulmasta seurasimme hyvin tarkasti mahdollisia tietoturvahyökkäyksiä ja niiden vaikutuksia Kevan palveluihin ja lakisääteiseen toimintaan. Tietosuojan ja tiedonhallinnan osalta selvitettiin mahdollisia juridisia riskejä liittyen tietojen käsittelyyn ja siirtoihin. Varautuminen poikkeustilanteisiin ja -oloihin oli ja on edelleen tärkeää, sillä lakisääteisen tehtävän hoitamista eli eläketurvan toimeenpanoa ei voida keskeyttää missään olosuhteissa.

Tietoturvan osalta auditoimme ympäristömme sekä varmistimme varautumisemme mm. Kyberturvakeskuksen ohjeita huoltovarmuuskriittisille toimijoille -ohjeen mukaan. Harjoittelimme myös kybertilanteen käsittelyä ja siitä toipumista. Läpikävimme tiedonhallintalain vaatimukset tietoturvalle sekä teimme toimenpidelistan vaatimusten täyttämiseksi.

Tiedonhallinnan osalta asiakirjahallinnossa valmisteltiin uusien asianhallintajärjestelmien (Armas-järjestelmät) käyttöönottoa. Vuonna 2022 keskityttiin HR-Armaksen, SijoitusArmaksen ja UudenArmaksen (koko Kevaa koskeva) järjestelmien rakentamiseen vaatimusten mukaisiksi.

2.1 Tietoriskit

Tiedon käsittelyyn kohdistuu aina riskejä, olipa tiedonkäsittely sähköistä tai manuaalista. Kevassa käsitellään paljon dataa ja tietoa, joka on kriittistä sekä Kevan toiminnalle että 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. Tietoriskien kartoittaminen ja niiden mitigointi on osa Kevan päivittäistä työtä.

3 Tiedonhallinta Kevassa

Kevan tiedonhallinta tähtää siihen, että kevalaisilla ja Kevan asiakkailla sekä sidosryhmillä on käytössään oikeellista, ajantasaista ja oikea-aikaista tietoa ja Keva käsittelee tietoa tietoturvallisesti, tietosuojavaatimusten sekä lainsäädännön vaatimusten mukaisesti.

Tiedonhallintapolitiikassa vuodelta 2020 linjataan pääpiirteet tiedon ja asiakirjojen elinkaaresta Kevassa. Tiedonhallintamallia, jolla täytetään tiedonhallintalain mukaisia velvoitteita, päivitettiin 2022. Tiedonohjaussuunnitelmassa (TOS) määrätään tarkemmin eri asiakirjaryhmien säilytysajoista ja -paikoista. Osa asiakirjojen ja tietojen säilytysajoista määräytyy eri säädöksien perusteella. Muutoin säilytysaikoja harkitaan tarkoituksen mukaan, huomioiden henkilötiedot ja niitä koskevat tietosuojaperiaatteet kuten tietojen minimoinnin ja säilyttämisen ainoastaan käyttötarkoitusta varten tarvittavan ajan.

3.1 Asiakirjahallinta ja julkisuusperiaate

Kevassa sovelletaan viranomaisen julkisuudesta annettua lakia (621/1999, julkisuuslaki), jonka mukaan lähtökohtaisesti viranomaisen asiakirjat ovat julkisia. Julkisuuslain 24 §:n nojalla kuitenkin osa asiakirjoista ja niiden sisältämästä tiedosta on salassa pidettäviä.

Asianhallinnan diaariin merkittäviä asioita vuonna 2022 oli 305 kappaletta. Julkisuuslain nojalla tehtyjä tietopyyntöjä oli 27 kappaletta. Tietopyyntöjä saapui muun muassa eläkeindeksiin liittyen, mikä selittyy poikkeuksellisilla indeksikorotuksilla, joista Keva tiedotti myös itse. Myös kansanedustajien sopeutumisrahan saajista tehtiin tietopyyntöjä. Saajien nimet ovat julkisia, mutta tarkemmat tiedot etuuden määrästä sen sijaan eivät ole julkisia (KHO 19.10.2006/2746).

3.2 Robotiikan käyttö asianhallinnassa

Ensimmäinen robottiprosessi otettiin käyttöön Kevassa 2018. Roope Robotti ja Elmeri Robotti toimivat tuotantopuolella ja Roosa Robotti testipuolella. Kevan robotiikkaprosessit ajetaan ohjelmistorobotiikkaympäristössä. Robotit ovat käytössä eläke- ja työelämäpalveluissa, sijoitustoiminnossa, rahoituksen ja

talouden toiminnossa sekä yleisjohdossa. Roboteilla pyritään vähentämään manuaalityön määrää ja sen myötä tehostamaan toimintaa. Uusia prosesseja otettiin käyttöön Kevan sijoitusten riskin estimoinnissa. Näitä työkaluja sekä tulosdataa hyödynnetään mm. sijoitusstrategiayksikössä.

Robotit hoitavat tehtäviä, joiden suorittamisessa ihmistyön käyttö ei ole tarkoituksenmukaista. Toiminnot, kuten materiaalien ja asiakirjojen siirtäminen järjestelmästä toiseen, automaattisten muistutusten lähettäminen sekä datan vertailu eri tarkoituksissa, ovat kustannustehokkaampia toteuttaa robotiikan avulla. Poikkeustilanteita syntyy myös robotiikan käytössä. Poikkeamia monitoroidaan ja niihin reagoidaan asianmukaisesti.

Toiminto	Tehtävät 2020	Poikkeamat 2020	Tehtävät 2021	Poikkeamat 2021	Tehtävät 2022	Poikkeamat 2022
Eläke- ja työelämäpalvelut	20816	2794	23662	2923	35778	4189
Sijoitustoiminto	944	13	3287	64	17455	8767
Yleisjohto	994	206	1504	210	1559	192
Rahoituksen ja talouden toiminto	426	217	187	35	198	38

1 Tilasto Robotiikkatehtävät ja poikkeamat v. 2020–2022

3.3 Automaattinen päätöksenteko Kevassa

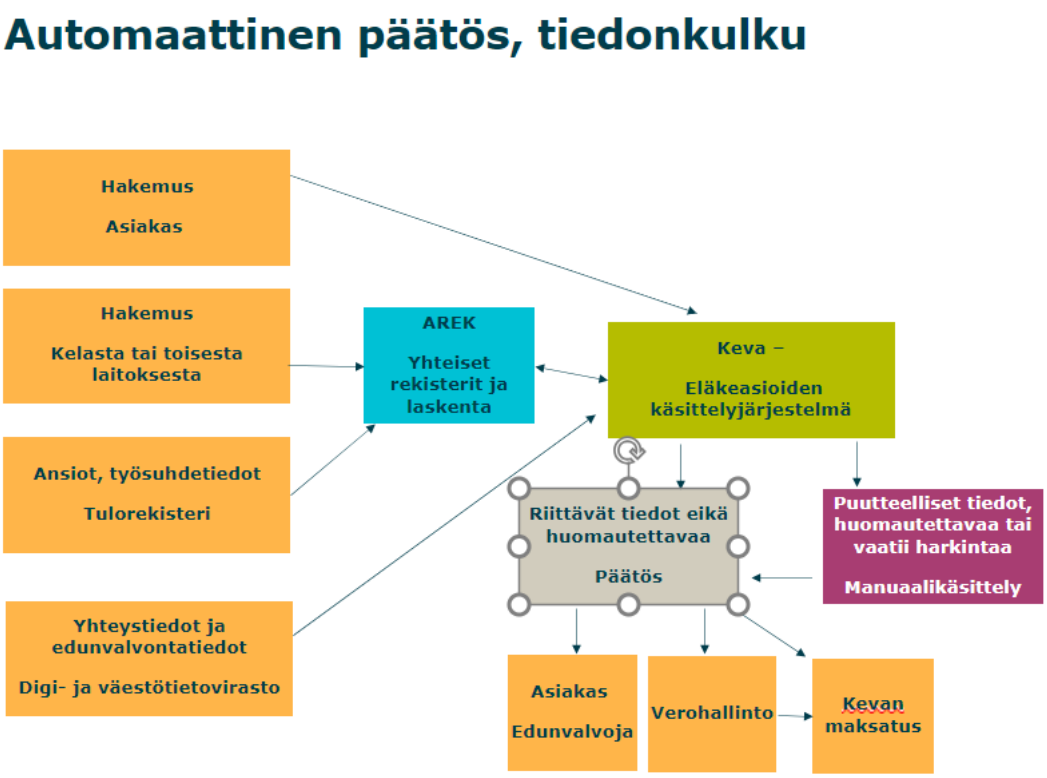
Keva osallistui lausunnoin vuonna 2022 lakimuutoksen valmisteluun, jossa hallintolakiin (434/2002) lisättiin 8 b luku koskien automaattista päätöksentekoa. Hallintolain 53 e 2 momentin muotoilussa lainsäätäjä päätyi muotoiluun, jonka mukaan viranomainen voi ratkaista automaattisesti asian, johon ei sisälly seikkoja, jotka edellyttävät tapauskohtaista harkintaa, tai johon sisältyvät tapauskohtaista harkintaa edellyttävät seikat virkamies tai muu asian käsittelijä on arvioinut. Ratkaisemisen on perustuttava sovellettavan lain ja etukäteisen harkinnan

perusteella laadittuihin julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n 16 kohdassa tarkoitettuihin käsittelysääntöihin.

Kevassa automaattiset päätökset voivat kohdistua asioihin, jotka voidaan ratkaista ilman tapauskohtaista harkintaa säänte-lyssä esitettyjen laskentasääntöjen mukaan. Esimerkiksi van-huuseläkepäätöksen voi saada automaattisesti ratkaistuna, mi-

käli eläkekäsittelyjärjestelmän käytössä on ajantasaiset ja riittävät tiedot. Eläkeasioiden käsittelyjärjestelmään tulee tietoja niin vakuutetulta itseltään kuin Arekin kautta Kelasta tai muista työeläkelaitoksista. Arek on työeläketoimijoiden yhteinen tietojärjestelmä- ja rekisteritoimittaja. Lisäksi tietoja vakuutetun ansioista sekä työsuhteista (mm. alkamis- ja päättymispäivämäärät) tulee Arekin kautta Tulorekisteristä. Henkilö- ja perhesuhdetiedot sekä tieto edunvalvonnasta tulee suoraan Digi- ja väestötietovirastosta.

Mikäli näiden tietojen perusteella järjestelmä ei nosta huomautettavaa ja päätös voidaan laskea saaduilla tiedoilla, päätös muodostuu automaattisesti ja siitä tieto lähtee vakuutetull~~a~~ea, Kevan maksatukseen sekä Verohallintoon. Automaattisen käsittelyn keskeyttävää huomautettavaa voi olla esimerkiksi hakijan pyyntö harkinnanvaraisesta palkantarkistuksesta (jonka tekee asiantuntija Kevassa) tai Arekin laskenta huomaa, ettei hakija ole hakenut kaikkia etuuksia, joihin tämä olisi oikeutettu. Automaattisessa asian käsittelyssä korostuu tarve ajantasaiselle ja paikkansapitävälle tiedolle, myös muissa tietojärjestelmissä kuin Kevan omissa.



Kuva 1 Automaattinen päätöksenteko - tiedonkulku

4 Tietosuoja Kevassa

4.1 Tietosuojan tilanne ja kehittämiskohteet

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. Tietosuojavastaava suoritti CIPP/E- koulutuksen (Certified Information Privacy Professional/Europe) ja sai sertifioinnin. Tietosuojavastaava on osallistunut myös muihin ulkopuolisiin koulutukseen kuten Tietosuojapäivään ja sen etkoihin 27.-28.1.2022.

Vuonna 2022 tietosuojaa koskevia sopimuspohjia tarkastettiin ja muokattiin paremmin vastaamaan erilaisia käyttötarkoituksia. Esimerkiksi SaaS-palvelujen (Software as Service) tietosuoja-asiat seikat vaativat sopimusasiakirjoilta eri asioiden huomioimista kuin konsultti- ja koulutuspalvelujen hankinnat.

Tietosuojavastaava osallistui myös automaattista päätöksentekoa koskevan lakihankkeen kommentointiin ja siihen varautumiseen. Myös henkilötunnuksen uudistamishanketta valmisteltiin. Ainakin henkilötunnusten välimerkkiuudistus eteni suunnitellusti. Digi- ja väestötietovirastolta haetaan uudistettua lupaa käsitellä turvakieltoasiakkaiden henkilötietoja sekä päivitettiin turvakiellon alaisten henkilötietojen käsittelyohjetta.

Kevassa valmisteltiin myös uuden GRC-ohjelman hankintaa, jota tietosuojavastaavan on tarkoitus tulevaisuudessa käyttää esimerkiksi riskitapahtumien raportointiin. Tämä hankintaprojekti jatkuu vuonna 2023 ja tietosuojavastaava osallistuu projektiin aktiivisesti. Tietosuojavastaava osallistui myös Kevan Code of Conduct -asiakirjan päivittämiseen. Vuoden aikana kevalaiset konsultoivat tietosuojavastaavaa muun muassa evästeasioissa ja tietosuojakysymyksissä koskien uusia sisäisiä palveluja sekä hankintoja. Tiivis yhteistyö compliance officereiden, riskienhallintapäällikön sekä tietoturvapäällikön kanssa jatkui vuonna 2022.

4.2 Rekisteröidyn 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.

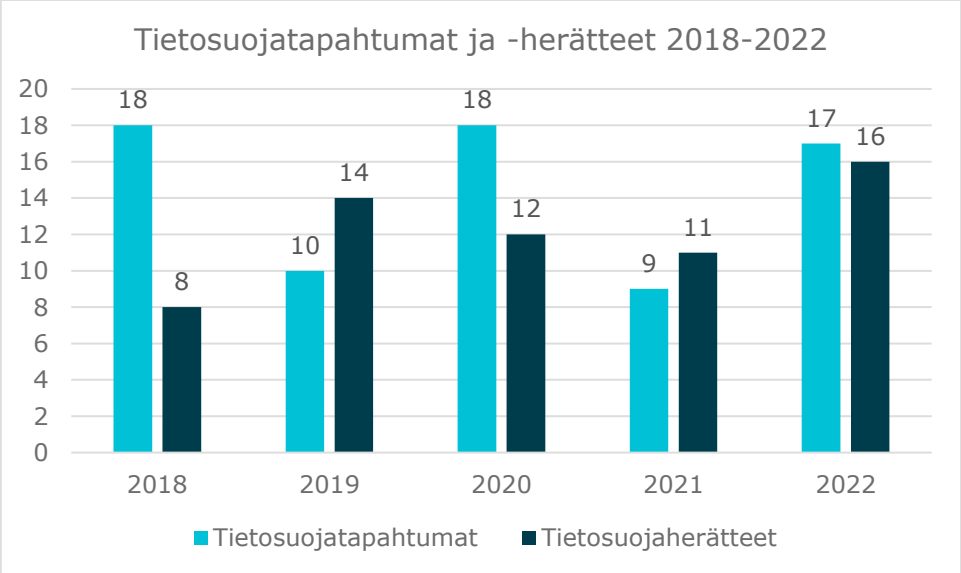
Rekisteröidyillä on tietosuoja-asetuksen mukainen oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään/ei käsitellä. Jos henkilötietoja käsitellään, rekisteröidyllä on oikeus saada pääsy henkilötietoihinsa sekä oikeus virheellisten tietojen oikaisemiseen tai tietojen poistamiseen. Oikeus poistamiseen ei ole kuitenkaan ehdoton, Kevassa esimerkiksi lakisääteisen tehtävän hoitamiseksi on tarpeen

käsitellä vakuutettujen henkilötietoja eikä tietoja voida poistaa. Vuonna 2022 omien tietojen tarkastamista pyydettiin seitsemän kertaa, joista kahteen pyyntöön ei voitu vastata, koska pyytäjä ei antanut riittävästi tietoja, jotta pyynnön tekijän henkilöllisyydestä voitaisiin varmistua.

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 kohdistuvista poikkeamista. Tietosuojatapahtuma on tilanne, jossa loukkaus on jollakin asteella tapahtunut. Tietosuojaheräte on signaali, jossa varsinaista loukkausta ei ole tapahtunut. Tapahtumat ja herätteet vuosina 2022 koskivat eläkevakuutettujen tietoja. Tietosuojatapahtumissa voi olla kyse inhimillisestä virheestä tietojen käsittelyssä tai tekninen virhe tietojärjestelmässä. Tyypillisesti kyse on yksittäisen asiakirjan tallennus- ja näkyvyysvirheestä tietojärjestelmässä.

Tietosuojavaltuutetulle tehtiin vuonna 2022 ilmoitus tietoturvaloukkauksesta kahdeksan kertaa. Tietoturvaloukkauksista ilmoitetaan myös rekisteröidylle, mikäli loukkaus todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille.



4.3 Kehittämiskohteet

Tiedonhallintalain vaatimusten läpikäynnissä havaittiin, että seuraavien tietoriskien osalta täytyy suunnitella toimenpiteitä:

- kasautumisvaikutus suorien sql-kyselyiden osalta
- säilytyksen rajoittaminen Kevan tietojärjestelmissä olevien tietojen osalta
- käsittelyn turvallisuus, erillistä tietoriskiarviointia ei ole tehty
- käsittelyn turvallisuus, dokumentoidaan erityishenkilötietoryhmien suojaustoimenpiteet.

Vuonna 2023 yhteistyötä ja viestintää Kevan sisällä on tarkoitus edelleen jatkaa ja kehittää. Tietosuojavaikutusten arviointeihin on tarkoitus panostaa vuonna 2023 silmällä pitäen Kevan pilvistrategiaa ja pilveistämisprojektia.