Tampereen ammattikorkeakoulu

Henkilötietojen tietoturva asian-ajotoimistossa

Rekisteröidyn oikeussuojakeinojen käyttö tietoturva-loukkaustilanteessa

Hilla Salo

OPINNÄYTETYÖ
Toukokuu 2020

Liiketalous
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalous
Oikeudellinen asiantuntijuus

HILLA SALO:
Henkilötietojen tietoturva asianajotoimistossa
Rekisteröidyn oikeussuojakeinojen käyttö tietoturvaloukkaustilanteessa

Opinnäytetyö 54 sivua, joista liitteitä 2 sivua
Toukokuu 2020

Asianajotoimiston tietoturvatoimenpiteiden kehittämishankkeen yhteydessä heräsi kysymyksiä tietosuoja-asetuksen myötä tulleista uusista vaatimuksista tietoturvan suhteen. Kehittämishankkeeseen päätettiin sisällyttää tiedonhaku sen selvittämiseksi, mitä oikeudellisia seuraamuksia tietoturvaloukkauksella voi olla asianajotoimistolle, asianajajalle ja siinä työskenteleville. Tämä opinnäytetyö toteutettiin tietoturvahankkeen tiedonhakuvaiheen toteuttamiseksi. Toimeksiantajana oli tamperelainen asianajotoimisto, Asianajotoimisto Kari Miettinen & Co Oy.

Työn tavoitteena oli selvittää rekisteröidyn mahdollisuudet käyttää oikeussuojakeinoja rekisterinpitäjää vastaan. Tarkoituksena oli selvittää, missä ja miten säädetään asianajotoimiston tietoturvasta ja mitä seurauksia sillä on, mikäli tietoturvasta ei huolehdita asianmukaisesti. Tietoturva sisältyy yleisen tietosuoja-asetuksen henkilötietojen käsittelyn periaatteeseen *eheys ja luottamuksellisuus* (TSA artikla 25 f). Lisäksi tietoturvaan liittyvää sääntelyä on kansallisessa laissa ja asianajajaliiton säännöissä. Rekisteröidyn asemassa olevan oikeussubjektin oikeussuojakeinoja tietoturvaloukkauksen suhteen tarkasteltiin sekä prosessuaalisesta että taloudellisesta näkökulmasta. Lisäksi työssä tarkasteltiin yleisesti asianajotoimiston tietoturvaa koskevaa sääntelyä. Opinnäytetyö toteutettiin lainopillisena tutkimuksena.

Työn tulosten avulla toimeksiantajan tietoturvaprojektia suunnattiin enemmän osoitusvelvollisuuden täyttämiseen ja konkreettisten tietoturvatoimenpiteiden suhteen päädyttiin käyttämään ja konsultoimaan IT-tukea. Työn oikeudellinen viitekehys koostui aiheeseen liittyvästä lainsäädännöstä, oikeuskirjallisuudesta, lausunnoista, tutkimuksista sekä viranomaislähteistä.

Asiasanat: Tietoturvaloukkaus, Rekisteröidyn oikeussuojakeinot, tietosuoja-asetus, asianajotoimisto

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Option of Legal Expertise

HILLA SALO:
Security of Personal Data in an Attorney's Office
Data Subject's Possibilities to Exercise Judicial Remedies in Case of Personal Data Breach

Bachelor's thesis 54 pages, appendices 2 pages
May 2020

The thesis was commissioned by Attorney's office Kari Miettinen & Co Oy. This study examined the possible legal consequences of personal data breach to an Attorney's office, attorney and its employees. Study carried out a part of the office's development project of data security.

The objective of the study was to explore the data subject's possibilities to exercise judicial remedies against controller. Purpose was to gather information on how attorney's office's personal data protection is regulated and what the legal consequenses of failing it are.

Data protection is part of the GDPR's principle 'integrity and confidentiality' (GDPR article 5). Data protection is also regulated by multiple national regulations. Judicial remedies were examined in both processual and economical point of views. The thesis exploited a juridical method.

As a conclusion of the study the data security project was oriented more to perform 'accountability' instead and IT-support was consulted on questions about appropriate technological protection. Main sources were legislation, legal literature, official's statements and studies.

Key words: Personal data breach, Data subject's juridial remedies, General data protection regulation, Attorneys's office

SISÄLLYS

ERITYISSANASTO JA LYHENTEET

Henkilötieto

kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. (Yleinen tietosuoja-asetus, 4 artikla)

Henkilötietojen käsittely

toiminto tai toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. (Yleinen tietosuoja-asetus, 4 artikla)

Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin (Yleinen tietosuoja-asetus, 4 artikla)

Rekisterinpitäjä

luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti, (Yleinen tietosuoja-asetus, 4 artikla)

Henkilötietojen käsittelijä

luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (Yleinen tietosuoja-asetus, 4 artikla)

Kolmas osapuoli

luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä ja henkilö,

joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena, (Yleinen tietosuoja-asetus, 4 artikla)

ETL Esitutkintalaki 22.7.2011/805

HOL Laki oikeudenkäynnistä hallintoasioissa 5.7.2019/808

OAL Oikeusapulaki 5.4.2002/257

ROL Laki oikeudenkäynnistä rikosasioissa 11.7.1997/689

TSA Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. (Tietosuoja-asetus, myös GDPR)

1 JOHDANTO

Opinnäytetyössä selvitetään mitä seurauksia tietoturvaloukkauksella voi olla asianajotoimistolle. Työn tavoitteena on selvittää asiakkaan käyttämien oikeussuojakeinojen seuraukset asianajotoimistolle henkilötietojen tietoturvaloukkaustilanteessa. Asianajotoimistossa työskentelevien tulee tietää prosessien kulku sekä olla tietoinen asiakkaan oikeuksista, oikeusturvasta ja oikeussuojakeinoista. Työssä tutkitaan oikeussuojaprosesseja, joihin turvautumalla rekisteröity turvaa tietosuojaoikeuksiaan mutta joiden kautta toisaalta rekisterinpitäjän vastuu toteutetaan. Työssä keskitytään tietoturvaan, joka on yksi konkreettinen osa yleistä tietosuoja-asetusta. Tietoturva sisältyy yleisen tietosuoja-asetuksen henkilötietojen käsittelyn periaatteeseen eheys ja luottamuksellisuus (TSA artikla 25 f)[1].

Kipinä työhön syntyi asianajotoimiston tietoturvaprojektin yhteydessä kysymyksestä: ”Mitä seurauksia henkilötietojen tietoturvaloukkauksella voi asianajotoimistolle olla? Onko mahdollista välttyä sanktioilta toteuttamalla tietosuoja-asetuksen tarkoittamat tekniset ja organisatoriset toimenpiteet tietoturvan kannalta? Mitä muita mahdollisia seurauksia tietoturvaloukkauksella voi olla?” Yleistä tietosuoja-asetusta on sovellettu 25.5.2018 lähtien ja sitä täydennettiin kansallisella lainsäädännöllä säätämällä tietosuojalaki (1050/2018), joka tuli voimaan 1.1.2019. Tietosuoja-asetus toi *tietoturvan* näkökulmasta laajan ilmoitus- sekä osoitusvelvollisuuden. Yleisen tietosuoja-asetuksen voimaantulon yhteydessä uutisoitiin laajasti sen mahdollistamista merkittävistä, jopa 20 miljoonan euron suuruisesta tai 4 % yrityksen vuotuisesta globaalista liikevaihdosta hallinnollisesta sanktiosta[2]. Yleistä tietoisuutta ei kuitenkaan tavoittanut se, mitkä ovat mahdolliset muut, paljon todennäköisemmät, voimassa olevien lakien mukaiset sanktiot henkilötietojen tietoturvaloukkauksen yhteydessä.

---

[1]Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (Tietosuoja-asetus (TSA))

[2] Pitkänen, 2016

Koska tietoturvaa säädellään edelleen monissa eri laissa, työn tutkimusongelmaa oli mielekästä tutkia rekisteröidyn oikeussuojakeinojen näkökulmasta. Tällä tavoin työssä päästiin niiden prosessien lähteille, joissa rekisterinpitäjän vastuu käytännössä toteutuu. Esimerkiksi tietosuojarikoksissa ja tietosuojavaltuutetun hallinnollisessa menettelyssä on useimmiten rekisteröity alullepanijana. Tietoturvaan liittyvissä oikeussuojaprosesseissa seuraukset riippuvat käsittelevän viranomaisen toimivaltuuksista. Tietoturva kuuluu *eheyden ja luottamuksellisuuden* periaatteeseen[3]. Tietosuoja-asetus ei anna vastauksia varmoihin tietoturvatoimiin, joilla voisi ennakoida tietosuoja-asetuksen noudattamisen ja sanktioilta säästymisen. Sen sijaan merkittävämpää tietosuoja-asetuksen kannalta on osoitusvelvollisuuden täyttäminen[4]. Lisäksi asianajoalaa koskee asianajajalain mukaisesti laaja salassapitovelvollisuus, joka sitoo sekä asianajajaa että hänen palveluksessaan olevia (Laki asianajajista (Asianajajalaki 496/1958) 5 c § (626/1995)). Työssä pyrittiin löytämään myös vastaus siihen, mikä vaikutus on sillä, että asianajajan toimintaa velvoittaa sekä tietosuoja-asetuksen luottamuksellisuuden periaate että lakisääteinen salassapitovelvollisuus.

Tietosuojavaltuutetun prosessi alkaa joko viranomaisen itsensä aloitteesta tai rekisteröidyn valituksesta[5] tai ilmoituksesta. Rikosoikeudellinen menettely alkaa rekisteröidyn tutkintapyynnöstä. Näin ollen kysymyksenasettelu tarkentui ja työssä päädyttiin etsimään vastauksia kolmeen seuraavaan kysymykseen:

1. Mitä oikeussuojakeinoja asiakkaalla on käytössään voimassa olevan lainsäädännön mukaan henkilötietojen tietoturvaloukkaustilanteessa?
2. Minkälainen kynnys rekisteröidyllä on oikeussuojakeinojen käyttämiseen? Mikä on eri oikeusturvaprosessien kesto, saavutettavuus ja hinta?
3. Mitä sanktioita asianajotoimistolle / asianajajalle voi aiheutua tietoturvaloukkauksesta, kun rekisteröity käyttää oikeussuojakeinojaan?

---

[3] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (Tietosuoja-asetus (TSA)) 5 artikla

[4] Korpisaari P. ym 2018, 311

[5] Huom. TSA:n tarkoittama rekisteröidyn tekemä valitus rekisterinpitäjän tai tietojenkäsittelijän toiminnasta tulee erottaa hallintopäätöksestä tehtävästä, hallinto-oikeudellisesta valituksesta. Tähän rekisteröidyn valitusoikeuteen viitataan tietosuojavaltuutetun teksteissä usein sanalla ilmoitus, kyseessä on käännöskukkanen.

Tietosuoja-asetuksessa säädetään rekisteröidyn päivitetyistä ja uusista oikeuksista, tietosuojavaltuutetun valtuuksista sekä rekisterinpitäjän velvollisuuksista. Tietosuoja-asetuksen sovellettavaksi tulon jälkeisen ensimmäisen yhdeksän kuukauden aikana tietosuojavaltuutetun toimistolle ilmoitettiin 2 700 henkilötietojen tietoturvaloukkausta[6]. Merkittävin tietoturvauhka vuoden 2018 viestintäviraston toimintakertomuksessa on yksityisiin ja organisaatioihin kohdistuva Office-365 -tunnusten kalastelu[7]. Kalastelun kohteena olevat Microsoftin palvelut ovat käytössä useissa keskisuurissa ja suurissa organisaatioissa, myös monissa asianajotoimistoissa.

1.1 Tutkimusmenetelmät ja oikeudellisen tiedon haku

Tässä työssä vastausta tutkimuskysymyksiin etsitään lainopillisesti, tutkimalla voimassaolevaa oikeutta. Lainopilla on perinteisesti ollut kaksi tehtävää: tulkinta ja systematisointi. Lainopillisessa tutkimuksessa metodit ovat ennen kaikkea tulkinnan menetelmiä, joilla selvitetään voimassaolevien oikeusnormien sisältöä. Lainopilla esitetään kahdenlaisia väitteitä oikeusnormeista, normikannanottoja ja tulkintakannanottoja. Lainoppi tutkii sitä, mikä on voimassaolevaa oikeutta ja mikä merkitys laista ja muista oikeuslähteistä löytyvällä materiaalilla on. Normikannanotot ovat väitteitä siitä, mitkä oikeusnormit kuuluvat voimassaolevaan oikeuteen. Tulkintakannanotossa edetään pidemmälle ja väitetään jotain kyseisen oikeusnormin sisällöstä.[8]

Lainopillisessa tutkimuksessa tutkitaan oikeudellisia tekstejä. Tämän työn tutkimusaineiston muodostaa työssä käytetyt oikeudelliset tekstit, joita ovat lainsäädäntö, lain esityöt kuten hallituksen esitykset ja valiokuntamietinnöt, oikeuskäytäntö, viranomaisten päätökset ja ohjeistukset sekä oikeuskirjallisuus. Lisäksi työssä hyödynnetään asianajaliiton valvonta-asiakirjoja, ohjeita sekä sääntöjä.

---

[6] Tietosuojavaltuutetun toimisto 2019.
[7] Viestintävirasto 2019, 4
[8] Hirvonen 2011, 22

Asianajajaliitto on julkisoikeudellinen yhdistys, joka hoitaa julkista hallintotehtävää harjoittaessaan asianajajien kurinpitoa. Edellä mainitut tekstit muodostavat tutkimusaineiston.[9]

Työssä käytetään tulkintametodeina objektiivista sekä historiallista tulkintaa. Historiallisessa tulkinnassa selvitetään lainsäätäjän tarkoitus, jota selvitetään ensisijaisesti lain esitöistä. Lainsäätäjän tarkoitus on lainopin tulkinnan kautta muodostettu. Objektiivisessa tulkinnassa lakitekstin ilmaisulle annetaan vakiintuneeseen oikeuskäytäntöön perustuva objektiivinen tai auktoriteettiperusteinen tulkinta.[10]

Tutkimusaineistoa valitessa ja tulkintaa tehdessä on lainopissa otettava huomioon oikeuslähdeoppi. Oikeuslähdeopin mukaan oikeuslähteet jaetaan Suomessa vakiintuneesti kolmeen luokkaan, vahvasti ja heikosti velvoittaviin sekä sallittuihin oikeuslähteisiin. Vahvasti velvoittavia oikeuslähteitä ovat laki ja maantapa. Heikosti velvoittavia lainvalmistelutyöt ja tuomioistuinratkaisut ja sallittuja lähteitä ovat oikeustiede, oikeusperiaatteet, moraali ja reaaliset argumentit.[11]

Oikeuslähdeoppi antaa myös vastauksen tulkinnassa käytettyjen oikeuslähteiden hierarkiaan. Oikeuslähdeopin avulla työssä on voitu tarkastella lähteiden painoarvoa ja vaikuttavuutta tutkimuskysymykseen. Oikeuslähdeoppi jaottelee oikeuslähteiden hierarkian seuraavasti:

1) Hierarkkisesti ylempitasoinen normi syrjäyttää alempitasoisen, esimerkiksi EU-oikeuden normi kansallisen lainsäädännön normin (lex superior derogat legi inferiori).
2) Uudempi normi syrjäyttää aiemmin säädetyn normin, jollei uudemman normin voimaanpanoa koskevat määräykset muuta sano (lex posterior derogat legi priori).
3) Erityisnormi syrjäyttää yleisnormin (lex specialis derogat legi generali).
4) Uudempi yleisnormi ei syrjäytä aiempaa erityisnormia, ellei toisin ole säädetty (lex posterior generalis non derogat legi priori speciali).[12]

---

[9] Hirvonen 2011, 23
[10] Hirvonen 2011, 33
[11] Hirvonen 2011, 42-43
[12] Hirvonen 2011, 34-45

Työn pääasiallisia lähteitä ovat EU-tasoinen lainsäädäntö, kansallinen lainsäädäntö, viranomaislähteistä lain valmistelutyöt sekä ohjeet ja päätökset.

1.2 Aiempi tutkimus

Tietosuoja-asetus -aiheesta on laadittu lukuisia AMK-opinnäytetöitä. Theseus-tietokannasta löytyy hakusanalla *tietosuoja-asetus* 1 986 AMK-opinnäytetyötä, hakusanalla *tietosuoja-asetus organisaatio* löytyy 961 AMK-opinnäytetyötä, hakusanalla *tietoturvaloukkaus oikeussuoja* löytyy 4 opinnäytetyötä, joista yksi käsittelee rekisteröidyn oikeussuojakeinoja tietoturvaloukkaustilanteessa. Suurin osa tehdyistä opinnäytetöistä käsittelee uutta tietosuoja-asetusta organisaation sisäisten käytänteiden näkökulmasta. Opinnäytetyöt on tehty pääosin selvittämään, mitä vaikutuksia tietosuoja-asetuksella on organisaation sisäisiin käytäntöihin ja kuinka tietosuoja-asetuksen voimaantuloon tulee organisaatiossa valmistautua. Sanktioiden tai asiakkaan oikeussuojakeinojen näkökulmasta löytyy vähemmän tutkimusta. Työtä, jossa käsiteltäisiin tietosuoja-asetuksen vaikutuksia tietoturvaloukkaustilanteessa asianajotoimiston kannalta ei ole julkaistu ennen tätä työtä. Edellä mainittu työ, joka käsittelee rekisteröidyn oikeussuojakeinoja, on julkaistu 2019. Siinä käydään läpi potilaan oikeussuojakeinot terveydenhuoltoalalla tietoturvaloukkaustilanteessa. Yksikään työ, jota tämän opinnäytetyön valmistumisen myötä oli julkaistu, ei esitellyt asiaa seuraamusten näkökulmasta tai esitellyt tietosuojan oikeusturvaprosesseja.[13]

Asiantuntija-artikkeleita on vielä hyvin rajallisesti saatavilla. Tietosuoja-asetus muutti kansallista sanktiojärjestelmäämme enemmän hallinnollisten sanktioiden suuntaan. Tästä aiheesta kirjoittaa Mikael Koillinen Defensor Legis -lehden tietosuojan ja immateriaalioikeuden teemanumerossa 4/2016. Tekstissä käsitellään Eu-oikeuden vaikutusta sanktioihin ja hallinnollisen sanktioinnin ongelmia perusoikeuksien näkökulmasta. Erityisesti syyllisyysperiaatteen kannalta kirjoittaja näkee hallinnollisen sanktioinnin olevan ongelmallista.[14]

[13] Theseus 2020
[14] Koillinen 2016, 574-576

2 ASIANAJOTOIMISTO REKISTERINPITÄJÄNÄ

Rekisterinpitäjä on tietosuoja-asetuksen mukaan luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. (TSA 4 artikla)

Asianajotoimistot käsittelevät asiakkaiden henkilötietoja toimeksiantojen hoitamiseksi. Asianajotoimistot toimivat asetuksen mukaisina rekisterinpitäjinä, kun taas esimerkiksi asianajajat ja asianajoassistentit henkilötietojen käsittelijänä. Asianajajat kuluvat asianajajaliittoon, joka on asianajajalakiin perustuva julkisoikeudellinen yhteisö. Asianajajia ja heidän toimintaansa säädellään asianajajalaissa (Laki asianajajista 496/1958). Ammatinharjoittaminen mahdollistuu täyttämällä asianajajaliiton vaatimukset. Asianajajan toimintaa valvoo asianajajaliiton valvontalautakunta sekä oikeuskansleri[15].

Rekisterinpitäjällä on velvollisuus huolehtia tietoturvasta ja rekisteröidyllä on oikeus tietojensa luottamuksellisuuteen. Rekisterinpitäjän vastuulla on asianmukaiset tekniset ja organisatoriset toimet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan yleistä tietosuoja-asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Rekisterinpitäjän tulee käsitellä henkilötietoja ennaltaehkäisevästi (TSA 24 artikla). Tietoturva sisältää tietojen luottamuksellisuuden, eheyden ja saatavuuden sekä usein lisäksi osaksi tietoturvaa luetaan todennus, vastuullisuus ja kiistämättömyys[16].

Tietosuoja-asetus ei anna tarkkaa määritelmää mitkä toimenpiteet ovat riittäviä tietosuoja-asetuksen vaatimusten noudattamiseksi. Tietoturvatoimenpiteiden ja menettelyjen osalta organisaatioille jää paljon liikkumavaraa tietosuoja-asetuksen myötä. Tämä asettaa organisaatioille paljon vastuuta. Tietosuoja-asetuksen

[15] Oikeuskanslerinvirasto 2020
[16] Korpisaari P. ym, 2018, 306

40 ja 42 artikloissa tarkoitetut hyväksytyt käytännesäännöt ja sertifiointimekanismit ovat mahdollisia työkaluja sen osoittamiseksi, että asetuksen vaatimuksia tietoturvan osalta noudatetaan.[17]

Tietosuoja-asetuksen mukaisia sanktioita rekisterinpitäjälle voi langeta tietoturvaloukkauksesta johtuen elinkaaren eri vaiheissa niin ennakoinnin, käsittelyn, reagoinnin, tiedottamisen kuin osoitusvelvollisuuden täyttämisen vaiheissa. Sanktioita määrätään prosesseissa, joissa rekisteröidyllä on merkittävä rooli alullepanijana (TSA 77 artikla).

Suomen oikeudenkäyttöjärjestelmä koostuu riippumattomasta tuomioistuimesta, syyttäjälaitoksesta, ulosottoviranomaisesta tuomioiden täytäntöön panijana, rikosseuraamuslaitoksesta vankeusrangaistusten toimeenpanijana, valtion oikeusaputoimistoista, oikeusavusta sekä itsenäisestä asianajajakunnasta. Asianajajat toimivat tiiviissä yhteistyössä oikeuslaitoksen kanssa ja ovat olennainen osa oikeussuojan toteuttamista Suomessa. Siinä missä julkisen hallinnon toimintaa ohjaa julkisuusperiaate, asianajajien toimintaa ohjaa ensisijaisesti salassapitoperiaate. Asianajotoimistolla on yleisen tietosuoja-asetuksen mukaisesti samat velvollisuudet kuin muillakin yrityksillä, jotka käsittelevät henkilötietoja. Henkilötietojen käsittelylle tulee aina olla lainmukainen peruste[18]. Tietosuoja-asetuksen lisäksi asianajajien toiminnan kannalta oleellista on asianajajien ja heidän avustajien lakisääteinen salassapitovelvollisuus.[19]

EU:n yleistä tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. Tietosuoja-asetus on sinällään suoraan sovellettavaa lainsäädäntöä koko EU:n alueella. Tietosuoja-asetusta sovelletaan sellaiseen henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista sekä sellaisten henkilötietojen käsittelyyn, jotka muodostavat rekisterinosan tai joiden on

[17] Korpisaari P. ym 2018, 311
[18] Tietosuojavaltuutetun toimisto 2019
[19] Tietoturvaohjeet 2019, Oikeus.fi tuomioistuimet 2020, oikeus.fi valtion oikeusaputoimistot 2018

tarkoitus muodostaa rekisterin osa. Tietosuoja-asetuksen täydentämiseksi säädettiin kansallinen tietosuojalaki (1050/2018), jonka tarkoituksena oli erityisesti valtuuttaa kansallinen tietosuojaviranomainen. (TSA 2 ja 3 artiklat)

Asianajajalaissa salassapitovelvollisuus sisältää asianajajaa sekä hänen apulaistaan koskevan kiellon ilmaista luvattomasti yksityisen tai perheen salaisuutta tai liikesalaisuutta, josta on saanut tehtävässään tiedon (asianajajalain 5 c §). Säädökseen on sisällytetty myös rangaistussäännös salassapitovelvollisuuden rikkomisesta. Rangaistussäännökset löytyvät rikoslain (39/1889) 38 luvun 1 ja 2 §:stä. Näin ollen asianajajaa velvoittaa yleisen tietosuoja-asetuksen luottamuksellisuusmääräysten lisäksi salassapitosäännös, jonka rikkominen on kriminalisoitu.

Tietosuoja-asetuksen noudattamista valvoo Suomessa tietosuojavaltuutettu. Tietosuojavaltuutetun toimisto antaa lisäksi ohjeita ja neuvontaa tietosuoja-asioissa niin rekisterinpitäjille kuin rekisteröidyillekin tietosuoja-asetuksen sekä tietosuojalain antamien toimivaltuuksien nojalla. (Tietosuojalaki 1050/2018 8 §, TSA)

2.1 Henkilötietojen käsittely

Henkilötiedolla tarkoitetaan tietosuoja-asetuksessa kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity), liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. *Käsittelyllä* tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. (TSA 4 artikla)

Asianajotoimisto käsittelee henkilöstönsä ja toimeksiantoasiakkaansa henkilötietoja, vastapuolen henkilötietoja, asianosaisten henkilötietoja sekä yritystoimeksiantojen kautta muitakin henkilötietoja kuten toimeksiantoyritysten työntekijöiden tietoja. Rekisteröity saa tärkeää tietoa tietojensa käsittelystä, kun rekisterinpitäjä täyttää tietosuoja-asetuksen vaatimukset ja noudattaa informaatiovelvollisuuttaan (TSA 12 artikla). Hyvin laadittu organisaation sisäinen, tietosuoja-asetuksen 30 artiklan edellyttämä seloste käsittelytoimista antaa valmiudet informaatiovelvollisuuden täyttämiselle.

Kun rekisterinpitäjä täyttää tietosuoja-asetuksen III luvun mukaiset vaatimukset läpinäkyvyydestä ja toimitettavista tiedoista, saa rekisteröity kattavan kuvan, millä perusteella, miten ja mihin hänen tietojaan käytetään, luovutetaan ja tallennetaan. Aikaisemman henkilötietolain vaatimuksen mukaista rekisteriselostetta ei enää voimassa olevan lain mukaan vaadita. Nykyinen informaatiovelvoite täytetään jakamalla tietosuoja-asetuksen mukainen selvitys tietojenkäsittelystä. Selvitys käsittelystä, kun tiedot on saatu rekisteröidyltä itseltään, laaditaan noudattamalla tietosuoja-asetuksen artiklan 13 vaatimuksia tiedoksiannon sisällöstä. Tiedoksianto sisältää tietoja aiemmasta rekisteriselosteesta, mutta on laajempi erityisesti informoinnin läpinäkyvyyden ja rekisteröidyn oikeuksien käyttämisen osalta. Uutena vaatimuksena on myös tiivis esitysmuoto, läpinäkyvyys, helppo ymmärrettävyys, saatava muoto ja yksinkertainen kieli (TSA 12 artikla).

Asianajotoimistojen henkilötietojen käsittelyperusteita ovat yleisimmin tietosuoja-asetuksen 6 artiklan a, b, c, d ja f kohdat:

a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä (vastapuolen henkilötietojen käsittelyn lakisääteinen perusta)
c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi; (esimerkiksi konkurssin pesänhoitaja tai tuomioistuimen määräämä pesänjakaja)
d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa

edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.[20]

2.2 Riskiperusteinen lähestymistapa henkilötietojen käsittelyssä

Rekisterinpitäjän tulee tehdä objektiivinen riskiarviointi käsittelyn riskitason määrittelemiseksi. Rekisterinpitäjän ja henkilötietojen käsittelijän on turvallisuuden ylläpitämiseksi ja asetuksen säännösten vastaisen käsittelyn estämiseksi riskien arvioimisen lisäksi toteutettava toimenpiteitä näiden riskien lieventämiseksi. Toimenpiteenä esitetään esimerkiksi salaus, jonka avulla luottamuksellisuus voitaisiin varmistaa. Riskiarviointiin esitetään tietosuojavaltuutetun verkkosivuilla malli, jonka toteuttamiseksi rekisterinpitäjän tulee ensiksi muodostaa selkeä käsitys sen omasta henkilötietojen käsittelystä (seloste käsittelytoimista). Tämä luotu käsitys toimii pohjana riskiarvioinnille. Riskiarvioinnin tavoitteena on tunnistaa käsittelystä aiheutuvat riskit rekisteröidyn oikeuksille ja vapauksille. Riskiarvioinnin tärkeä osa on arvio haitan vakavuuden ja toteutumisen todennäköisyydestä. Mitä korkeampi riskin ja siitä aiheutuvan haitan vakavuus ja toteutumisen todennäköisyys ovat, sitä suurempi merkitys on rekisterinpitäjän tekemillä teknisillä ja organisatorisilla keinoilla henkilötietojen käsittelyssä. [21]

Vaikutusten arviointi[22] on osa henkilötietojen käsittelyn riskiperusteista lähestymistapaa. Vaikutusten arviointi tietosuoja-asetuksen vaatimalla tavalla ei ole aina pakollista. Vaikutusten arvioinnilla tarkoitetaan tietosuoja-asetuksessa tietojenkäsittelytoimien vaikutusten arviointia, jonka vähimmäisvaatimukset on määritelty asetuksessa. Vaikutusten arviointiin kuuluu:

- kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta
- arvio ... rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä

[20] TSA 6 artikla käsittelyn periaatteista
[21] TSA johdannon kohdat 73 ja 83, tietosuoja.fi/arvioi riskit
[22] DPIA, Data protection impact assessment, 35 artikla

- sunnitellut toimenpiteet ”riskeihin puuttumiseksi” ja sen osoittamiseksi, että ”tätä asetusta on noudatettu”. (TSA 35 artiklan 7 kohta, johdanto-osan 84 ja 90 kappale, tietosuojavaltuutetun toimisto[23].)

Vaikutusten arviointi vaaditaan vain, jos käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta *korkean riskin*. Vaikka vaikutustenarvioinnin ehdot eivät täyttyisikään, rekisterinpitäjällä on edelleen velvollisuus toteuttaa toimenpiteitä, joilla hallitaan rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä[24]. Vaikutusten arviointi vaaditaan erityisesti silloin, kun

- henkilötietojen käsittelyssä käytetään uutta teknologiaa
- käsitellään laajamittaisesti rikostuomioita, rikkomuksia tai erityisiä henkilötietoryhmiä, kuten terveystietoja, etnistä alkuperää, poliittisia mielipiteitä, uskonnollista vakaumusta tai seksuaalista suuntautumista
- henkilön henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn avulla, järjestelmällisesti ja kattavasti, ja arvio johtaa päätöksiin, joilla on oikeusvaikutuksia tai jotka muuten vaikuttavat henkilöön merkittävästi
- yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajamittaisesti.[25]

Näin ollen tulee huomioida, että vaikutusten arviointi ei koske tietoturvallista toimintaa suoraan, vaan arvioinnissa tulee ottaa huomioon laajasti tietosuoja-asetuksen suomia oikeuksia, kuten oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. Huolimatta siitä, edellyttääkö tietosuoja-asetus organisaatiossa vaikutusten arvioinnin itsearviointityökalun käyttöä, on rekisterinpitäjän omaksuttava riskiperusteinen lähestymistapa henkilötietojen käsittelyyn. Tämä tarkoittaa käytännössä, että rekisterinpitäjillä on edelleen yleinen velvollisuus toteuttaa toimenpiteitä, joilla hallitaan rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Riskiperusteisella arvioinnilla tunnistetaan, milloin käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin.[26]

Henkilötietojen käsittelyä koskevia, velvoittavia periaatteita on yhteensä kuusi:

a) lainmukaisuus, kohtuullisuus ja läpinäkyvyys
b) käyttötarkoitussidonnaisuus

---

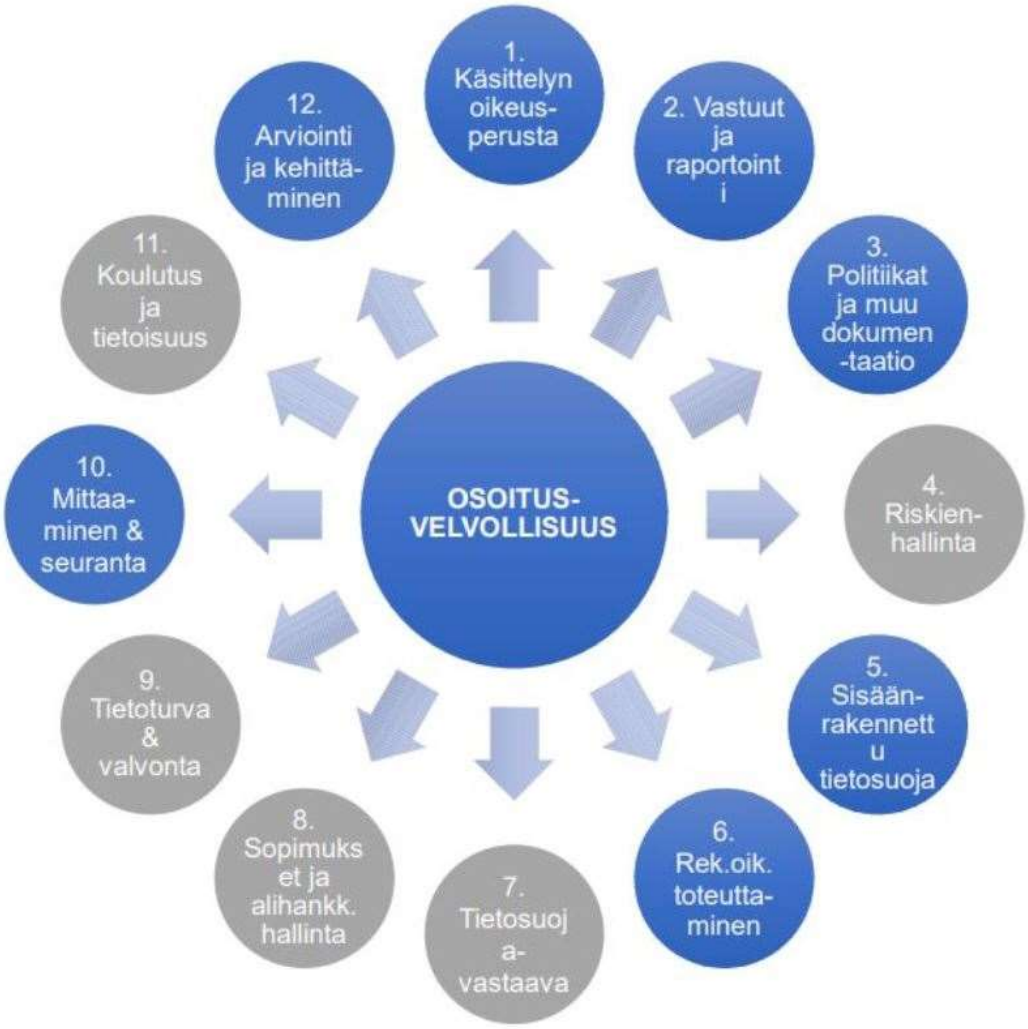
[23] Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski" 2017, 19
[24] Korpisaari ym. 2018, 330
[25] Tietosuojavaltuutetun toimisto 2020
[26] Korpisaari ym. 2018, 330

c) tietojen minimointi
d) täsmällisyys
e) säilytyksen rajoittaminen
f) eheys ja luottamuksellisuus. (TSA artikla 5)

Viimeinen kohta, eheys ja luottamuksellisuus koskee erityisesti tietoturvallista henkilötietojen käsittelyä:

> (henkilötietoja) -- on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus). (TSA artikla 5 kohta 1)

Tietoturvallista toimintaa koskee osana tietosuoja-asetusta osoitusvelvollisuus. Rekisterinpitäjä vastaa osoitusvelvollisuudesta ja sen on pystyttävä osoittamaan, että asianmukaisia teknisiä ja organisatorisia toimia on käytetty varmistamaan, että henkilötietoja käsitellään tietoturvallisesti tietosuoja-asetuksen vaatimusten



mukaisesti (TSA 5 artikla, kohta 2). Osoitusvelvollisuutta käsitellään laajasti tietosuojavaltuutetun ohjeissa. Tietosuojavaltuutetun ja valtiovarainministeriön yhteistyöryhmän koulutusmateriaaleissa julkaistu kooste osoitusvelvollisuuden laajuudesta on tiivistys siitä, mitä kaikkea osoitusvelvollisuus koskee (Kuva 1).

Kuva 1. Osoitusvelvollisuus rekisterinpitäjän velvollisuuksien ytimessä.[27]

Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuutena on uusin tekniikka ja toteuttamiskustannukset huomioiden toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi (TSA 5 artikla). Tietoturvallisen toiminnan keinoja ovat tietosuoja-asetuksessa esitetysti:

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten
   a) henkilötietojen pseudonymisointi ja salaus;
   b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
   c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
   d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.
2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.
3. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.
4. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita. (TSA artikla 32)

[27] Rekisterinpitäjän velvollisuuksien toteuttaminen 2017, 4

Tietosuoja-asetuksen määräykset tietoturvan suhteen lähtevät siitä, että velvoitettavien toimenpiteiden laajuuden suhteen tulee huomioida uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Tietosuojariskiä arvioitaessa olisi otettava huomioon henkilötietojen käsittelyyn liittyvät riskit, kuten siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy, mikä voi aiheuttaa etenkin fyysisiä, aineellisia tai aineettomia vahinkoja. Tietoturvan kannalta kevyemmät turvamekanismit riittävät vähäisempien riskien torjumiseen, kun taas yksityisyydelle vakavimpien riskien torjuntaan on käytettävä kaikki keinot, joita uusin tekniikka tarjoaa. Turvamekanismit suhteessa tietoturvallisuuden tavoitteisiin ja niiden tarpeellisuus voidaan perustaa riskiarvioon, jota käsitellään TSA 25 artiklan yhteydessä.[28]

Loukkauksen tai haitan vakavuus	Vakava	Matala riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Matala riski
		Kaukainen	Mahdollinen	Hyvin mahdollinen
		Loukkauksen tai haitan todennäköisyys		

Kuva 1. Tunnistetun riskin vakavuuden ja todennäköisyyden arviointi.[29]

Tietoturvallisesta toiminnasta on vastuussa rekisterinpitäjä, ja tämän on varauduttava mahdollisiin tietoturvaloukkauksiin. Varautuminen tapahtuu laatimalla riskiarvio ja toimintaohjeet mahdollisia tietoturvaloukkaustilanteita varten. Rekisterinpitäjän on pystyttävä reagoimaan nopeasti tietoturvaloukkauksiin. Rekisterinpitäjän on arvioitava, minkä tasoinen riski voi aiheutua tietoturvaloukkauksesta sen kohteena olevalle henkilölle.[30]

[28] Korpisaari ym. 2018, 308 sekä yleinen tietosuoja-asetus, johdannon kohta 73 ja 83
[29] Tietosuojavaltuutetun toimisto 2019
[30] Tietosuojavaltuutetun toimisto 2019

2.3 Asianajajaliiton tietoturvaohjeet

Asianajajaliitto julkaisee sääntöjä, ohjeita sekä oppaita, jotka ovat joko velvoittavia tai laadultaan suosituksia. Asianajajaliitto käyttää julkaisemiaan ohjeita ja sääntöjä valvonta-asioiden ratkaisujen perustana, oppaat täydentävät ohjeita ja ovat käytännön apuna toiminnan järjestämiseksi niin, että ohjeita noudatetaan asianajajien toiminnassa. Asianajajaliiton hyvää asianajajatapaa koskevat ohjeet ovat jäseniä velvoittavia:

> Jäsenen tulee rehellisesti ja tunnollisesti täyttää hänelle uskotut tehtävät sekä kaikessa toiminnassaan noudattaa hyvää asianajajatapaa ja jäsenten noudatettavaksii vahvistettuja ohjeita.[31]

Asianajajaliiton ohjeita ja sääntöjä sovelletaan valvonta-asioissa. Asianajaliiton tapaohjeet sisältävät vaatimukset muun muassa toiminnan perusarvoista ja yleisistä periaatteista[32]. Luottamuksellisuuden periaate sisältää salassapidon ja vaitiolovelvollisuuden määräykset:

> Asianajaja ei saa luvattomasti ilmaista sellaista yksityisen tai perheen salaisuutta taikka liike- tai ammattisalaisuutta, josta hän tehtävässään on saanut tiedon (salassapitovelvollisuus). Asianajaja ei saa myöskään luvattomasti ilmaista muita tietoja, joita hän on tehtävää hoitaessaan saanut tietää asiakkaasta ja tämän oloista (vaitiolovelvollisuus).[33]

Lisäksi ohjeissa on velvoite ajallisesti rajoittamattomasta salassapitovelvollisuudesta, josta voi vapautua vain sen vapauttamana, jota salassapito- ja vaitiolovelvollisuus suojaa, tai:

1. siihen on laista tai asianajajaliiton säännöistä johtuva velvollisuus;
2. se on välttämätöntä asianajajan puolustautuessa itseensä kohdistuvilta vaatimuksilta; tai
3. se on asianajajan asiakkaaltaan olevan saatavan perimiseksi välttämätöntä.[34]

---

[31] Oikeusministeriön päätös yleisen asianajajayhdistyksen sääntöjen vahvistamiseksi (Suomen asianajajaliiton säännöt, muut. viim. 2.4.2019/439)
[32] Hyvää asianajajatapaa koskevat ohjeet 2012, 1
[33] Hyvää asianajajatapaa koskevat ohjeet 2012, 3
[34] Hyvää asianajajatapaa koskevat ohjeet 2012, 14

Lisäksi tapaohjeissa on määräys tietoturvallisesta toiminnasta. Asianajotoimiston toiminnasta suhteessa valvontalautakuntaan on vastuussa asianajaja:

> Asianajajan on huolehdittava toimiston tietoturvallisuudesta siten, etteivät sivulliset pääse luvatta tutustumaan asiakkaiden tietoihin.[35]

Lisäksi asianajajaliitto on päivittänyt yleisen tietosuoja-asetuksen voimaantulon jälkeen hyvää asianajatapaa koskevan ohjeensa tietoturvallisesta toiminnasta. Tämä ohje tuli voimaan asianajajia velvoittavana 1.6.2019. Ohjeessa määrätään yksityiskohtaisesti tietojen salauksesta ja toimintatavoista, joilla luottamuksellisuus tietoturvallisten toimenpiteiden avulla voidaan varmistaa. Ohjeessa on muun muassa määräykset säännöllisestä ulkoisesta tietoturva-auditoinnista yli 10 työntekijän asianajotoimistoissa.[36]

[35] Hyvää asianajajatapaa koskevat ohjeet 2012, 14
[36] Tietoturvaohje B 5.1 2019 **ks. Liite 1**

3 MIKÄ ON HENKILÖTIETOJEN TIETOTURVALOUKKAUS?

Henkilötietojen tietoturvaloukkaus voi olla joko luottamuksellisuuden, eheyden tai saatavuuden loukkaus tai näitä useampia kerralla. Luottamuksellisuuden loukkaustilanteessa tietoja paljastuu luvattomasti tai vahingossa. Eheyden loukkaus tarkoittaa henkilötietojen luvatonta vahingossa tapahtunutta muuttumista. Saatavuuden loukkauksella tarkoitetaan tilannetta, jossa henkilötiedot tai niihin pääsy luvattomasti tai vahingossa menetetään.[37]

> *Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietosuoja-asetuksen määritelmän mukaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin*. (TSA artiklan 4 kohta 12)

Tietosuojavaltuutetun toimisto tarkentaa määritelmää niin, että määritelmän loppuun on lisätty maininta ulkopuolisesta tahosta:

> Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.[38]

Tuhoamisella tarkoitetaan, ettei tietoja ole, tai että rekisterinpitäjä ei niitä voi hyödyntää. Häviämisellä tarkoitetaan, että tiedot saattavat olla edelleen olemassa, mutta rekisterinpitäjä on menettänyt kontrollin tai pääsyn niihin tai ne eivät enää ole rekisterinpitäjän hallussa, häviämisestä on kyse myös, kun kiristysohjelma on salannut joukon henkilötietoja tai rekisterinpitäjän salausavain kadonnut niin, että tietoihin ei päästä käsiksi enää. [39]

Henkilötietojen tietoturvaloukkauksen erottaa muista tietoturvaongelmista se, että sen seurauksena rekisterinpitäjä ei enää kykene vastaamaan siitä, että se

---

[37] Korpisaari ym. 2018, 314
[38] Tietosuojavaltuutetun toimisto, luettu 30.3.2020
[39] Korpisaari ym. 2018, 314

noudattaa TSA 5 artiklan mukaisia henkilötietojen käsittelyä koskevia periaatteita. Henkilötietojen tietoturvaloukkaukset kuuluvat tietoturvaongelmiin, kaikki tietoturvaongelmat eivät ole henkilötietojen tietoturvaloukkauksia.[40]

Tietosuojavaltuutetun toimisto on julkaissut verkkosivuillaan lukuisia ohjeita liittyen tietoturvalliseen toimintaan sekä tietosuoja-asetuksen tuomiin oikeuksiin ja velvollisuuksiin. Tietosuojavaltuutetun toimiston ohjeissa on havainnollistettu sitä, miten tietoturvapoikkeamat käytännössä ilmenee. Tietosuojavaltuutetun toimiston esimerkeissä ja ilmoituslomakkeella on kuvattu niin ulkoisia, että myös organisaation suoraan itse toiminnallaan aiheuttamia tietoturvapoikkeustilanteita:

hävinnyt tiedonsiirtoväline, kuten USB-tikku
varastettu tietokone
hakkerointi
haittaohjelmatartunta
kyberhyökkäys
tulipalo datakeskuksessa
tiliotteen postitus väärälle henkilölle.
kadonnut tai varastettu laite
kadonnut varastettu tai varomattomasti säilytetty asiakirja
kadonnut tai avattu lähetys
hakkerointi
haittaohjelma
tietojenkalastelu
henkilöiden tietoja sisältävien asiakirjojen varomaton hävittäminen
tahaton julkaiseminen
väärää rekisteröityä koskevien tietojen luovuttaminen
henkilötietojen lähettäminen väärälle vastaanottajalle
henkilötietojen luvaton luovuttaminen suullisesti
muu[41]

Tietoturvaloukkauksen mahdollisina seurauksina tietosuoja-asetuksessa pidetään luonnollisille henkilöille aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja, kuten omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintää, identiteettivarkaus tai petos, taloudellisia menetyksiä, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys tai muuta merkittävää taloudellista tai sosiaalista vahinkoa.[42]

---

[40] Korpisaari ym. 2018, 315
[41] Tietosuojavaltuutetun toimisto, 2019. Luettu 29.3.2020
[42] Yleisen tietosuoja-asetuksen johdannon kohta 85

Rekisterinpitäjän tulee toteuttaa kaikki tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että tietoturvaloukkaukset paljastuvat välittömästi[43]. Tietoturvaloukkauksen paljastumisen varmistamiseksi tietoturvakoulutus ja organisaation vastuut tulee olla selvillä. Tietoturvan osa-alueiden jaottelut toimivat apuna organisaatioille tietoturvariskien arvioinnissa ja koulutuksessa. Jaottelun avulla voidaan paikantaa riskikohdat tietoturvasta ja toisaalta havainnoida tietoturvapoikkeama välittömästi. Yksi esimerkki tietoturvajaottelusta on F-Securen julkaisemassa koosteessa. Sen mukaan tietoturvapoikkeamia voidaan tarkastella neljän eri haavoittuvuustekijän kautta, joita ovat päätelaitteet, ohjelmistot, käyttäjät ja verkot.[44]

Kuva 1. Tietoturvan fyysisen ja kyber- maailman rajapinta.[45]

Vahti-ohjeessa (2017) on kuvattu ulkoisen hyökkääjän aiheuttamien tietoturvapoikkeamien ilmenemistapoja ja seurauksia (Kuva 2). Seuraavasta kuvan taulukosta nähdään, että kolmannen osapuolen tekemät tietoturvaloukkaukset ilmenevät hyvin monilla eri tavoilla. Edellytyksenä havainnoinnille on, että organisaatio tuntee verkkojen järjestelmien normaalitoiminnan sekä tietojen ja tietokantojen normaalin sisällön ja käyttötavat.[46]

---

[43] Korpisaari ym. 2018, 318
[44] Guide to holistic cyber security, F-Secure 2019
[45] Kuva muokattu Guide to holistic cyber security, F-Secure 2019 tietojen pohjalta
[46] Tietoturvapoikkeamien hallinta 2017, 33

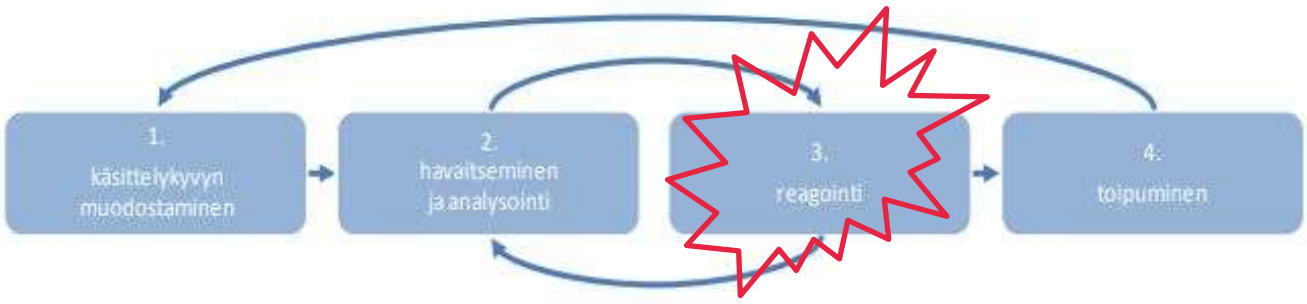
Haittakoodi	Virus	Ohjelmisto, joka on tarkoituksellisesti asennettu järjestelmään haitallisessa mielessä. Ohjelmiston aktivoituminen edellyttää yleensä käyttäjän toimia.
	Mato	
	Troijalainen	
	Vakoiluohjelma	
	Rootkit	
Tiedon kerääminen	Verkkoskannaus	Verkon rakenteen ja siinä olevien järjestelmien saavutettavuuden automaattinen tiedustelu
	Verkon nuuskinta	Verkon nuuskinnan tarkoituksena on seurata verkon liikennettä, valvoa sitä tai hankkia tietoja verkossa liikkuvista viesteistä ja salasanoista.
	Sosiaalinen tiedustelu	Ihmisten väliseen toimintaan perustuvaa tiedustelua, esimerkiksi esiintymistä puhelimessa jonain toisena henkilönä kuin itsenään tai valheellisesti jonkun organisaation edustajana luottamuksellisten tietojen hankkimiseksi.
Tunkeutumisyritys	Tunnetun haavoittuvuuden hyväksikäyttö	Tunkeutuminen tietojärjestelmään tai verkkoon yleisesti tunnetun haavoittuvuuden avulla
	Kirjautumisyritys	Palveluun pyritään tunkeutumaan kirjautumisen kautta hyödyntämällä esim. salasanalistoja
	Uusi tunkeutumistapa	Palveluun tai verkkoon tunkeutuminen ennalta tuntemattoman haavoittuvuuden avulla
Laiton tunkeutuminen	Pääkäyttäjätilin murto	Laiton tunkeutuminen verkkoon tai tietojärjestelmään. Tunkeutumisessa saatetaan hyödyntää haavoittuvuutta tai se voidaan myös tehdä paikallisesti. Sisältää myös bottiverkon osana toimimisen.
	Peruskäyttäjän tilin murto	
	Ohjelmiston murtaminen	
	Päätelaite osana bottiverkkoa	
Tiedon saatavuus-ongelma	Palvelunestohyökkäys	Saatavuusongelmat voivat johtua erilaisista palvelunestohyökkäyksistä tai esim. sähkönsyöttöön liittyvistä ongelmista.
	Sabotaasi	
	Sähkökatkos	
Tietoaineisto-turvallisuus	Luvaton pääsy tietoon	Tietoaineistoon liittyvät poikkeamat voivat liittyä mm. käyttäjätilin tai sovelluksen murtamiseen, verkon nuuskimiseen tai virheellisen konfigurointiin
	Tietojen luvaton muokkaus	
Petos	Palvelujen laiton käyttö	Palvelujen käyttö laittomaan tarkoitukseen
	Tekijänoikeusrikkomus	Lisensoimattoman sovelluksen asentaminen tai myyminen
	Toisena henkilönä esiintyminen	Identiteettivarkaudet
	Tietojen kalastelu	Salassa pidettävän tai sensitiivisen tiedon kalastelu
Haavoittuvuus	Järjestelmä on avoin väärinkäytölle	Järjestelmässä on paikkaamattomia haavoittuvuuksia tai järjestelmä on konfiguroitu virheellisesti
Joku muu	Kaikki muut poikkeamat, jotka eivät sovi muihin luokkiin	

Kuva 2. Tietoturvapoikkeamien luokittelu[47]

[47] Tietoturvapoikkeamien hallinta 2017, 37-38. Muokattu

3.1 Tietoturvaloukkauksen aiheuttamat toimenpiteet

Kun tietoturvapoikkeama havaitaan, se tulee ensisijaisesti dokumentoida tietosuoja-asetuksen vaatimusten mukaisesti. Dokumentoinnin tulee sisältää henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat tiedot (TSA artikla 33 kohta 5). Rekisterinpitäjällä ja henkilötietojen käsittelijällä on osoitusvelvollisuus siitä, että tarvittavat toimenpiteet vahingon rajaamiseksi on aloitettu välittömästi ja että organisaatiossa on toimittu ennaltaehkäisevästi ja riskiperusteisesti tietoturvan suhteen. Rekisterinpitäjän on tietoturvaloukkaustilanteessa tarkistettava, onko kaikki asianmukaiset tekniset ja organisatoriset toimenpiteet toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus. Lisäksi rekisterinpitäjän on osoitettava, että organisaatiossa on toimittu ennaltaehkäisevästi ja riskiperusteisesti tietoturvan suhteen. Tietoturvapoikkeaman hallintaprosessi voidaan jakaa neljään päävaiheeseen. Kuviosta 2 nähdään, että havaitsemisen ja reagoinnin vaiheet linkittyvät toisiinsa niin, että vaiheita toistetaan tarvittaessa. [48]



Kuva 3. Tietoturvapoikkeaman hallinnan 4 päävaihetta.[49] Muokattu

Reagointivaihe on havaitsemista ja alkuvaiheen analysointia välittömästi seuraava vaihe. Havaitsemisvaiheessa rekisterinpitäjä saa tiedon tietoturvapoikkeamasta. Reagointivaihe sisältää vahingon rajauksen ja alkuvaiheen analysoinnin, dokumentoinnin, tarpeellisten ilmoitusten laatimisen ja jakelun sekä vahingon riskienarvioinnin rekisteröidyn kannalta.[50]

---

[48] TSA johdannon kohta 87
[49] Tietoturvapoikkeamien hallinta 2017, 13
[50] Tietoturvaloukkaukset, Tietosuojavaltuutetun toimisto

Riskien arviointi tietoturvaloukkauksen tapahduttua tulee erottaa tietosuoja-asetuksen 35 artiklan mukaisesta vaikutusten arvioinnista. Vaikutusten arviointia voidaan hyödyntää tässä vaiheessa, mutta rekisterinpitäjän tulee kuitenkin tapauskohtaisesti arvioida kyseessä olevan yksittäisen tietoturvaloukkauksen seurauksia ja riskejä rekisteröidylle erikseen[51].

3.2 Ilmoitusvelvollisuus viranomaiselle ja rekisteröidylle

Tietoturvaloukkauksesta on ilmoitettava määrätyissä tapauksissa tietosuojavaltuutetulle ja myös rekisteröidylle (TSA 33 ja 34 artiklat). Aiemmin tällaista laajaa ilmoitus- ja osoitusvelvollisuutta ei ollut Suomen lainsäädännössä kuin teleyrityksillä, jotka oli velvoitettu ilmoittamaan tietomurrosta. Rekisterinpitäjällä on velvollisuus tietosuoja-asetuksen mukaan informoida tietoturvaloukkauksesta viranomaista ja tarvittaessa rekisteröityä. Kun loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille, henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa tietosuojavaltuutetulle 72 tunnin kuluessa (TSA artiklat 33 ja 34, TSL 8 §). Ilmoitusta voi toimittaa vaiheittain. Tietosuojaviranomaiselle toimitettavassa tiedoksiannossa on:

a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

b) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

c) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;

d) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi. (TSA artikla 32) [52]

---

[51] Korpisaari ym. 2018, 318

[52] HE 9/2018, 68, tietoyhteiskuntakaari 917/2014 275 §, nykyisin Laki sähköisen viestinnän palveluista 917/2014

Tietoturvaloukkauksesta ei tietosuoja-asetuksen mukaan tarvitse ilmoittaa, mikäli siitä ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Mikäli 72 tunnin aikamääreessä ei pysytä, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys. Sama velvollisuus koskee henkilötietojen käsittelijää[53]. Ilmoituksen voi tehdä tietosuojavaltuutetun verkkosivujen verkkolomakkeella, jossa on eritelty vaadittavat tiedot. Ilmoituksen voi tehdä myös vapaamuotoisesti, kuten turvapostilla kun ilmoitus sisältää salassa pidettäviä tietoja.[54]

Tietosuoja-asetuksessa säädetään ilmoitusvelvollisuudesta rekisteröidylle, kun henkilötietojen tietoturvaloukkaus on tapahtunut (TSA artikla 34). Rekisterinpitäjän tulee ilmoittaa rekisteröidylle tietoturvaloukkauksesta ilman aiheetonta viivytystä, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Kun ilmoitus henkilötietojen tietoturvaloukkauksesta rekisteröidylle tehdään, on ilmoituksessa kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava ainakin tietosuoja-asetuksen 33 artiklassa tarkoitetut tiedot ja toimenpiteet. Vähimmäisvaatimukset, kun rekisteröidylle tehdään ilmoitus:

1. ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;
2. kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;
3. kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.(TSA artiklat 33 ja 34)

Rekisteröidylle ei tietosuoja-asetuksen perusteella tarvitse ilmoittaa, jos jokin seuraavista edellytyksistä täyttyy:

a) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne

[53] TSA johdannon kohta 85
[54] Tietosuojavaltuutetun toimisto 2020

eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;

b) rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu;

c) se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla. (TSA 34, kohta 3)

Rekisterinpitäjän velvollisuus on arvioida rekisteröidylle aiheutunutta haittaa ja arvioinnin perusteella päätettävä rekisteröidyn informoinnista. Rekisteröidylle aiheutunutta haittaa voidaan arvioida tietosuojavaltuutetun toimiston julkaiseman kuusivaiheisen arviointiprosessin perusteella:

1. Tietoturvarikkomuksen tyyppi
Seuraukset voivat olla erilaisia esimerkiksi silloin, jos arkaluonteiset tiedot ovat vuotaneet internetiin, kuin silloin, jos henkilötietoja ei pääse käsittelemään tietojärjestelmävian vuoksi.

2. Henkilötietojen luonne, arkaluonteisuus ja määrä
Mitä arkaluonteisempaan tietoon tietoturvaloukkaus kohdistuu, sen suurempi riski siitä aiheutuu loukkauksen kohteena olevalle henkilölle. Myös rekisteröityä koskevien eri tietotyyppien yhdistelmä on usein arkaluonteisempi kuin yksittäinen rekisteröityä koskeva tieto. Kun tietoturvaloukkaus kohdistuu suureen määrään tietoja, myös seuraukset koskevat laajaa joukkoa.

3. Tunnistamisen helppous
On tärkeää arvioida sitä, kuinka helposti henkilöt ovat tunnistettavissa tietoturvaloukkauksen kohteena olevasta aineistosta joko suoraan tai välillisesti muiden saatavilla olevien tietojen avulla. Tunnistettavuuteen voi vaikuttaa muun muassa se, miten hyvin tiedot on salattu tai pseudonymisoitu.

4. Rekisteröidyn ominaisuudet
Tietoturvaloukkauksella voi olla vakavammat vaikutukset silloin, kun se kohdistuu lapsiin tai muihin haavoittuvammassa tai heikommassa asemassa oleviin.

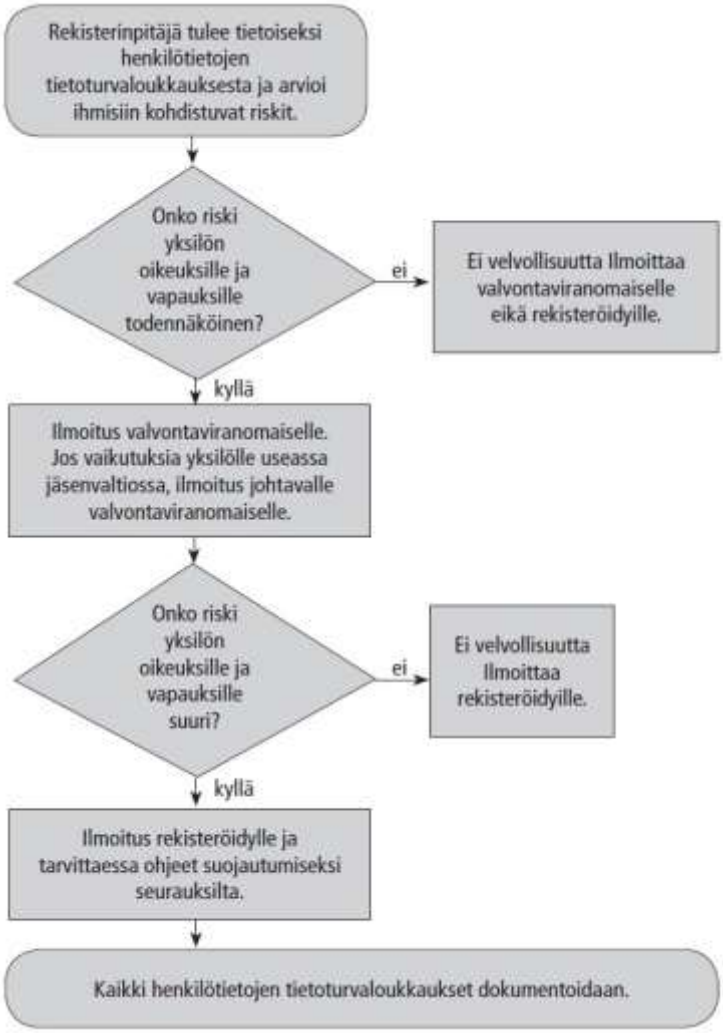
5. Rekisterinpitäjän ominaisuudet
Rekisterinpitäjän toimiala ja rooli voivat vaikuttaa siihen, millainen riski tietoturvaloukkauksesta aiheutuu. Esimerkiksi silloin, kun tietoturvaloukkaus tapahtuu sairaalan potilastietojärjestelmässä, on rekisteröidylle aiheutuva uhka todennäköisesti suurempi kuin silloin, kun tietoturvaloukkaus tapahtuu sanomalehden tilaajarekisterissä.
6. Tietovuodon seurauksien vakavuus

Tietoturvaloukkauksen seurausten voidaan katsoa olevan erityisen vakavia esimerkiksi silloin, kun siitä voi seurata identiteettivarkaus, petos, psyykkistä ahdistusta, nöyryytystä tai maineen menetys.

Myös se, kenen haltuun tiedot ovat joutuneet, voi vaikuttaa siihen, millaisia seurauksia on odotettavissa. Väärinkäytön todennäköisyys voi olla suurempi, jos tiedetään, että tiedot ovat päätyneet rikolliselle.

Kun arvioit tietoturvaloukkaukseen liittyvää riskiä, ota huomioon tietoturvaloukkauksesta mahdollisesti aiheutuvan seurauksen vakavuus ja todennäköisyys. Tietoturvaloukkaukseen liittyy sitä suurempi riski, mitä vakavampi seuraus on yksilön kannalta ja mitä todennäköisemmin se toteutuu. [55]

Seuraavassa kuviossa selvitetään, milloin tietoturvaloukkauksesta on ilmoitettava tietoturvaviranomaiselle ja rekisteröidylle.



Kuva 4. Henkilötietoloukkauksesta ilmoittaminen.[56]

[55] Tietosuojavaltuutetun toimisto 2020
[56] Korpisaari ym. 2018, 323

4 REKISTERÖIDYN OIKEUSSUOJAKEINOT

Oikeussuojakeinoilla tarkoitetaan niitä kansallisia ja kansainvälisiä (EU-tasoisia) keinoja, joilla asianosainen voi puolustaa lakisääteisiä oikeuksiaan ja vapauksiaan. Oikeus tehokkaisiin oikeussuojakeinoihin on vahvistettu EU- tasoisesti perusoikeuskirjan 47 artiklassa. EU-tasoinen lainsäädäntö sisältää määräyksen, että jäsenvaltioilla täytyy olla tehokkaan oikeussuojan takaava järjestelmä, jolla varmistetaan unionin oikeuden tehokas toteutuminen käytännössä. Yksilön kannalta se tarkoittaa sitä, että kansalaiset voivat vedota unionin oikeuteen kansallisissa tuomioistuimissa ja muissa kansallisissa viranomaisissa kansallisten menettelyiden mukaisesti. Euroopan Ihmisoikeussopimuksen (63/1999) 13 artiklan mukaan jokaisella, jonka ihmisoikeussopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä. Oikeussuojakeinojen tehokkuutta arvioidaan saatavuudella, vaikutuksilla, oikeudenkäynnin kestolla sekä yksilölle aiheutuvien kulujen näkökulmasta.[57]

Oikeudesta tehokkaiden oikeussuojakeinojen käyttöön säädetään Euroopan perusoikeuskirjan VI osaston, lainkäyttö, artiklassa 47:

> Jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava tässä artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa. Jokaisella on oikeus kohtuullisen ajan kuluessa oikeudenmukaiseen ja julkiseen oikeudenkäyntiin riippumattomassa ja puolueettomassa tuomioistuimessa, joka on etukäteen laillisesti perustettu. Jokaisella on oltava mahdollisuus saada neuvoja ja antaa toisen henkilön puolustaa ja edustaa itseään. Maksutonta oikeusapua annetaan vähävaraisille, jos tällainen apu on tarpeen, jotta asianomainen voisi tehokkaasti käyttää oikeutta saattaa asiansa tuomioistuimen käsiteltäväksi.[58]

Oikeussuojakeinon tehokkuutta arvioidaan sillä, milloin lainvoimainen ratkaisu annetaan, eikä ylimääräinen muutoksenhaku vaikuta kokonaiskeston tarkaste-

---

[57] HE 85/2012, Lainkirjoittajan opas 2013, 170-171
[58] Euroopan perusoikeuskirja 2000

luun. Ratkaisussaan *Kudla* v. Puola, EIT 2000 ihmisoikeustuomioistuin on katsonut tehokkaaksi oikeussuojakeinoksi sellaisen keinon, joka on myös käytännössä tehokas. Tehokkuus ei kuitenkaan riipu valittajalle myönteisen lopputuloksen varmuudesta. Tehokkuuden arviointiin vaikuttaa viranomaisen toimivalta ja sen tarjoamat oikeussuojatakeet. Kyseessä olevan viranomaisen ei tarvitse olla välttämättä lainkäyttöviranomainen (mm. poliisi, tietosuojaviranomainen ym.) Oikeussuojakeinoja ovat preventiivinen (ennalta ehkäisevä) keino, jolla voidaan estää oikeudenkäynnin viipyminen tai sen jatkuminen, tai reparatiivinen (jälkikäteen hyvittävä) keino, jolla voidaan asianmukaisesti hyvittää (”adequate redress”) jo tapahtunut loukkaus. Kudla-tapauksessa tällaista tehokasta keinoa ei ollut ollut valittajan käytettävissä, joten 13 artiklaa oli loukattu.[59]

Suomen perustuslakiin (731/1999) sisältyy yksityisen henkilön oikeusturvaa koskeva perussääntö oikeudesta saada asiaansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi sekä oikeussuojaperiaate, jonka mukaan valtion on annettava oikeussuojaa oikeudenloukkauksen kohteeksi joutuneelle. Oikeusturva on perusoikeus. Oikeusturvavaatimus liittyy perustuslain 21 §:n säännöksiin oikeudenmukaisesta oikeudenkäynnistä ja hyvästä hallinnosta:

> Jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. (PL 731/1999 21 §)[60]

Oikeusturvan toteutumisesta käytännössä vastaavat viime kädessä riippumattomat tuomioistuimet. Muita lainkäyttöviranomaisia ovat syyttäjät ja ulosottoviranomaiset. Myös oikeusavulla on keskeinen merkitys oikeusturvan toteutumisessa. Lainkäyttömenetelmät jaetaan kolmeen päätyyppiin käsiteltävän asian mukaan, oikeudenkäyntiin riita-asioissa, rikosasioissa ja hallintoasioissa.[61]

---

[59] HE 85/2012 ihmisoikeustuomioistuimen ratkaisusta *Kudla* v. Puola, EIT 2000
[60] Lainkirjoittajan opas 2013, 58
[61] Oikeusturvan toteutuminen, oikeusministerio.fi

Tietosuoja-asetuksessa säädetyn mukaisesti jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle asetuksen vastaisesta henkilötietojensa käsittelystä (TSA 77 artikla) sekä tehokkaisiin oikeussuojakeinoihin itseään koskevaa valvontaviranomaisen oikeudellisesti sitovaa päätöstä vastaan (TSA 78 artikla). Lisäksi rekisteröidyllä on oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan myös muuten kuin valittamalla tietosuojaviranomaiselle, jos hän katsoo, että hänen asetukseen perustuvia oikeuksiaan on loukattu sen takia, ettei hänen henkilötietojensa käsittelyssä ole noudatettu asetusta (TSA 79 artikla).

Tietosuoja-asetuksen ja kansallisten lakien tuomien oikeuksien kannalta tietoturvaan liittyen oikeusturva tarkoittaa sitä, että rekisteröity voi saattaa asiansa viranomaisen tai tuomioistuimen käsiteltäväksi. Oikeussuojakeinot, jotka ovat käytettävissä tietoturva-asioissa ovat ensisijaisesti kansallisia (TSA 79 artikla). Tietosuoja on yksilön perusoikeus perustuslain 10 §:n (yksityiselämän suoja), EU:n perusoikeuskirjan 7 ja 8 artiklan sekä Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan perusteella. Tietosuoja-asetuksella päivitettiin tietosuojaa erityisesti rekisteröidyn oikeuksien näkökulmasta. Rekisteröidyn tietojensaantioikeus parani ja oikeussuojakeinovaatimuksia parannettiin. Uuden tietosuoja-asetuksen ja sitä täydentämään laaditun kansallisen tietosuojalain perusteella rekisteröidyn oikeudet paranivat merkityksellisimmin niin, että rekisteröidystä tuli asianosainen tietoturva-asian hallintomenettelyssä ja rekisteröidyllä on valitusoikeus hallintopäätökseen, joka liittyy tämän henkilötietojen käsittelyyn. Oikeussuojakeinoihin rekisteröidyllä tulee tarve puuttua, kun tämän henkilötietojen tietoturvaa on loukattu. Se mistä rekisteröity saa tiedon henkilötietojen loukkauksesta sekä aiheutuuko tilanteesta vahinkoa, vaikuttavat prosessin valintaan. Rekisterinpitäjän kannalta tietoturvaan liittyvää riskiä voidaan ajatella vahingon toteutumistodennäköisyyden ja vahingon suuruuden tulona. Vahingon suuruuteen vaikuttavat paitsi suoraan menetettävien tietojen arvo myös esimerkiksi organisaation maineelle, brändille ja luotettavuudelle aiheutuva vahinko ja ulkopuolisille mahdollisesti maksettavat vahingonkorvaukset.[62]

[62] HE 9/2018, 56 sekä Korpisaari ym. 2018,5 310

4.1 Hallinnolliset oikeussuojakeinot

Rekisteröidyllä on lain mukaan oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan sitä koskevaa lainsäädäntöä. Menettelystä ei aiheudu kustannuksia rekisteröidylle. Mikäli pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti siitä syystä, että niitä esitetään toistuvasti, valvontaviranomainen voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea. Valvontaviranomaisen on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. (Tietosuojalaki 1050/2018 21 §, Tietosuoja-asetuksen 77 ja 57 artiklat)

Tietosuoja-asetuksen tarkoittama tietosuojaviranomainen Suomessa on tietosuojalain mukaisesti tietosuojavaltuutettu (Tietosuojalaki 8 § ja 24 §). Tietosuojavaltuutettu kollegioineen on hallintoviranomainen, jonka tulee toiminnassaan noudattaa hyvän hallinnon takeita, joista säädetään perustuslain 21 §:ssä:

1. Käsittelyn julkisuus
2. Oikeus tulla kuulluksi
3. Oikeus saada perusteltu päätös
4. Oikeus hakea muutosta (PL 21 §)

Tietosuojavaltuutettu on viranomainen, jonka on kaikessa toiminnassaan noudatettava lakia. Yleisesti viranomaisen hallintotoiminnasta säädetään hallintolaissa. Hallintolain (434/2003) 6 §:ssä säädetään hallinnon oikeusperiaatteet. Oikeusperiaatteet ovat yhdenvertaisuuden, tarkoitussidonnaisuuden, objektiviteetin ja suhteellisuuden periaatteet. Kun otetaan huomioon hallintolaissa säädetyt hallinnon oikeusperiaatteet, suhteellisuusperiaatteen mukaisesti hallinnollisen sanktio todennäköisesti tulee tietosuojavaltuutetun määräämänä sanktiona käyttöön vasta viimesijaisena keinona, keinovalikoima ollessa niin laaja. Hyvän hallinnon periaatteita ovat

1. palveluperiaate ja palvelun asianmukaisuus,
2. neuvontavelvollisuus,
3. hyvän kielenkäytön vaatimus ja

4. viranomaisten yhteistyövelvoite. (HL 6 §)

Tietosuojaviranomaisen tehtävistä ja valtuuksista säädetään tietosuoja-asetuksen 2 jaksossa *Toimivalta, tehtävät ja valtuudet*, artiklat 55-59. Tietosuojavaltuutetulla on laajat oikeudet tietojensaantiin tietosuoja-asioissa ja sen on valvottava tietosuoja-asetuksen soveltamista. Tietosuojaviranomaisen velvollisuudesta tutkia valituksia säädetään seuraavasti:

> Tietosuojaviranomaisen on valvottava tämän asetuksen soveltamista ja pantava se täytäntöön sekä käsiteltävä rekisteröidyn tai 80 artiklan mukaisen elimen, järjestön tai yhdistyksen tekemiä valituksia ja tutkittava siinä määrin kuin se on asianmukaista valituksen kohdetta ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä sekä tutkinnan tuloksista kohtuullisen ajan kuluessa, erityisesti jos asia edellyttää lisätutkimuksia tai koordinointia toisen valvontaviranomaisen kanssa. (TSA 79 artikla)

Kun rekisteröity epäilee yleisen tietosuoja-asetuksen mukaisia oikeuksiaan loukatun, tulee ensisijaisen yhteydenoton tietosuojavaltuutetun toimiston mukaan oltava suoraan rekisterinpitäjään, mielellään tietosuojavastaavaan. Mikäli rekisterinpitäjä ei ole määrännyt tietosuojavastaavaa, voi rekisteröity olla yhteydessä joko puhelimitse tai tietosuojavaltuutetun toimiston sivuilta löytyvän lomakkeen kautta rekisterinpitäjään. Rekisterinpitäjän tulee vastata yhteydenottoon 1 kuukauden aikana, kuitenkin viimeistään 3 kuukauden aikana erillisestä pyynnöstä. Tietosuojavaltuutettuun tulee ottaa yhteyttä vasta, jos rekisterinpitäjä on kieltäytynyt pyynnöstäsi tai ei anna vastausta määräajassa.[63]

Tietosuoja-asia tulee tietosuojavaltuutetun toimistoon vireille joko viranomaisen omasta aloitteesta tai rekisteröidyn aloitteesta. Hallintoasian vireilletulosta säädetään hallintolaissa. Osapuolia hallintomenettelyssä ovat tietosuojavaltuutettu (kollegioineen), rekisterinpitäjä/tietojen käsittelijä sekä tietosuoja-asetuksen myötä myös rekisteröity tai rekisteröidyn valtuuttama edustaja. Tietosuojavaltuutettu päättää vireilletulon jälkeen aloitetaanko menettely. Tietosuojavaltuutetun toimisto pyytää tarvittavat lausunnot ja selvitykset asian ratkaisemiseksi. Päätöksenteosta tietosuojavaltuutetun toimistossa säädetään hallintolailla, tietosuojalailla sekä asetuksella tietosuojavaltuutetun toimistosta. (TSA 58, 77 ja 80 artikla)

---

[63] Tietosuojavaltuutetun toimisto 2020

Tietosuojavaltuutettu toimittaa ilmoituksen asetuksen väitetystä rikkomisesta ja selvityspyynnön rekisterinpitäjälle (HL 5 ja 6 luku). Kuulemisten jälkeen tietosuojavaltuutettu voi antaa valituskelpoisen, kirjallisen hallintopäätöksen. Päätöksessä tiedotetaan toimenpiteistä, joita voivat olla varoitus, huomautus, määräys noudattaa rekisteröidyn pyyntöä, määräys saattaa käsittelytoimet asetuksen säännösten mukaisiksi, määrätä ilmoittamaan tietoturvaloukkauksesta rekisteröidylle, asettaa väliaikainen rajoitus käsittelylle, hallinnollinen sakko tai määräys tiedonsiirtojen keskeyttämisestä (TSA 58 artikla). Tietosuojavaltuutettu voi myös päättää, ettei toimenpiteisiin ole syytä ryhtyä.[64]

Tietosuojavaltuutetun hallintopäätöksestä voi valittaa hallinto-oikeuteen, ensimmäisenä asteena alueellinen hallinto-oikeus (TL 25 §, laki oikeudenkäynnistä hallintoasioissa (HOL, hallintoprosessilaki) 10 §)[65]. Kun rekisteröity valittaa tietosuojavaltuutetun päätöksestä hallinto-oikeuteen, ei hän enää hallinto-oikeuskäsittelyssä ole yleisesti asianosaisasemassa, vaan hänellä on tiedonsaantioikeus. Rekisteröity on asianosaisasemassa ainoastaan, mikäli hallinto-oikeuden päätöksellä katsotaan olevan välitön vaikutus rekisteröidyn oikeuteen[66]. Osapuolina hallinto-oikeudessa ovat rekisterinpitäjä/tietojenkäsittelijä sekä tietosuojavaltuutettu. Rekisteröidyn asemassa olevalla valittajalla on hallintoprosessilain mukainen oikeus saada tieto päätöksestä sekä käsittelystä, mutta rekisteröidyllä ei ole oikeutta antaa lausuntoa enää tässä vaiheessa[67]. Rekisteröidyllä on myös muut lakisääteiset oikeussuojakeinot käytössään tietosuojavaltuutettua kohtaan kuten kantelu oikeusasiamiehelle tai oikeuskanslerille. Mikäli tietosuojavaltuutettu ei käsittele tietosuoja-asiaa koskevaa valitusta tai ilmoita rekisteröidylle valituksen etenemisestä tai ratkaisusta kolmen kuukauden kuluessa, on rekisteröidyllä oikeus tehokkaisiin oikeussuojakeinoihin (tietosuoja-asetuksen 78 artikla). Tietosuojavaltuutetun toimiston keskimääräinen käsittelyaika on 38,4 päivää, hieman alle 1,5 kk.[68]

---

[64] HE 9/2018, 103
[65] aiemmin hallintolainkäyttölaki, kumottu lailla oikeudenkäynnistä hallintoasioissa 808/2019 (HOL, hallintoprosessilaki)
[66] Lakivaliokunnan lausunto 5/2018 vp, 21
[67] Lakivaliokunnan lausunto 5/2018 vp, 22
[68] Tietosuojavaltuutetun toimisto, vuosikertomus 2019, lakivaliokunnan lausunto 2018

Tietosuojalaissa säädetyn mukaan tietosuoja-asetuksessa säädetystä hallinnollisesta sanktiosta päättää tietosuojavaltuutetun ja apulaistietosuojavaltuutetun yhdessä muodostama seuraamuskollegio. Päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen kuten laissa oikeudenkäynnistä hallintoasioissa[69] säädetään (TL 25 §). Tietosuoja-asetuksen 83 artiklassa määrätyn hallinnollisen sakon määrää tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen yhdessä muodostama vähintään kolmijäseninen seuraamuskollegio (TL 24 §). Hallinto-oikeuden päätökseen muutosta saa hallintoprosessilain mukaisesti hakea vain, mikäli korkein hallinto-oikeus antaa valitusluvan. Hallinnollista seuraamusmaksua ei saa määrätä, jos on kulunut yli kymmenen vuotta siitä, kun rikkomus tai laiminlyönti on tapahtunut (TL 24 §). Jos rikkomus tai laiminlyönti on ollut luonteeltaan jatkuvaa, kymmenen vuoden määräaika lasketaan siitä, kun rikkomus tai laiminlyönti on päättynyt (TL 24.5 §). Hallintoprosessissa on lähtökohtana kaksiasteinen muutoksenhaku hallintotuomioistuimiin. Alueellisten hallinto-oikeuksien päätöksiin saa pääsääntöisesti hakea muutosta valittamalla korkeimmalta hallinto-oikeudelta. Muutoksenhakua on kuitenkin rajoitettu useissa asiaryhmissä säätämällä valitusluvasta tai valituskiellosta.[70]

4.2 Rikosoikeudellinen menettely

Rikos on laissa rangaistavaksi säädetty teko tai laiminlyönti. Rikosprosessi tulee vireille joko asianomistajan ilmoituksesta tai esitutkintaviranomaisen omasta aloitteesta. Esitutkintaa säätelee esitutkintalaki (ETL 805/2011). Esitutkintaviranomainen (poliisi) päättää esitutkinnan aloittamisesta. Tietoturvarikoksissa, kuten muissakin asianomistajarikoksissa toimitetaan esitutkinta vain, jos asianomistaja on ilmoittanut esitutkintaviranomaiselle tai syyttäjälle vaativansa rikokseen syyllistyneelle rangaistusta.[71]

Tutkintapyynnön tai rikosilmoituksen perusteella poliisiviranomainen suorittaa esitutkinnan, mikäli on syytä epäillä, että rikos on tehty. Asianomistajarikoksista,

---

[69] Aiemmin hallintolainkäyttölaki, kumottu lailla oikeudenkäynnistä hallintoasioissa 808/2019 (HOL, hallintoprosessilaki)
[70] HE 85/2012
[71] Virallisen syytteen alaiset rikokset ja asianomistajarikokset luettu 2020

joissa syyttäjä saa lain mukaan yleisen edun sitä vaatiessa nostaa syytteen asianomistajarikoksesta vaikkei asianomistaja vaatisikaan rikokseen syyllistyneelle rangaistusta, on esitutkinta syyttäjän pyynnöstä toimitettava (ETL 3:3 ja 3:4 §). Esitutkinnasta asia etenee syyteharkintaan, jossa syyttäjä tekee päätöksen syytteen nostamisesta. Syytteen nostaminen johtaa asian vireillepanoon käräjäoikeudessa. Mikäli syyttäjä ei nosta syytettä, jää asia sillensä. Asianomistajalla on kuitenkin oikeus nostaa syyte itse, jos virallinen syyttäjä on päättänyt jättää syytteen nostamatta (Laki oikeudenkäynnistä rikosasioissa (ROL) 1:14 §).

Edellytyksenä syytteen nostamiselle on se, että kyseinen teko on säädetty laissa rangaistavaksi eikä tekoa koskeva syyteoikeus ole vanhentunut[72]. Mikäli päätös syytteen nostamiseksi tehdään, etenee asia käräjäoikeuden käsiteltäväksi. Syyteharkinnan jälkeen syyttäjä ajaa syytettä tuomioistuimessa. Tuomioistuinkäsittelystä rikosasioissa säädetään laissa oikeudenkäynnistä rikosasioissa (689/1997). Asianosaisia menettelyssä ovat syytetty, syyttäjä ja asianomistaja. Tietosuojaasioissa tuomioistuimella on velvollisuus kuulla tietosuojavaltuutettua. Asianomistaja voi hakea muutosta asiassa annettuun ratkaisuun siitä riippumatta, onko hän käyttänyt asiassa puhevaltaa (ROL 1:14 §).

Rikoslaissa on säädetty rikosten määritelmät eli rikostunnusmerkistöt keskeisistä rikoksista[73]. Rikoslain (39/1889) 38 luvussa säädetään tieto- ja viestintärikoksista. Tietoturvaan ja tietojen käsittelijään liittyen luvussa on säädökset salassapitorikoksesta, rikkomuksesta viestintäsalaisuuden luokkauksen eri muodoista tietomurrosta sekä tietosuojarikoksesta (RL 38:1-9 §). Lisäksi rikoslain 24 luvussa on rangaistussäännökset yksityisyyden, rauhan ja kunnian loukkaamisesta[74]. Henkilötietojen tietoturvaloukkauksessa voi olla kyse esimerkiksi yksityiselämää loukkaavan tiedon levittämisestä[75]. Yksityiselämää loukkaavan tiedon levittämisen teonkuvauksena on oikeudeton toisen yksityiselämän tiedon, vihjauksen tai kuvan toimittaminen lukuisten ihmisten saataville siten, että teko on

[72] Linna 2019, 152
[73] Oikeusministeriö
[74] Kunnianloukkauksessa (RL 24: 9 §) on kyse valheellisen tiedon tai vihjauksen esittämisestä tai muusta halventamisesta. Yksityiselämää loukkaavan tiedon levittämisessä on kyse (RL 9:8 §) oikeudettomasta yksityiselämän tiedon, vihjauksen tai kuvan levittämisestä.
[75] Tietosuojavaltuutetun toimisto 2020

omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa (RL 24:8 §). Oikeushenkilö on rikosoikeudellisessa vastuussa ainoastaan törkeän kunnianloukkauksen osalta rikoksissa, jotka luetaan yksityisyyden, rauhan ja kunnian loukkaamiseen (RL 24: 12 §).

Rikosoikeudellinen vastuu poikkeaa muista rekisterinpitäjän vastuista. Oikeushenkilöllä, rekisterinpitäjällä ei ole rangaistusvastuuta tietosuojarikoksissa[76]. Rikosoikeudellinen vastuu tietosuojarikoksissa kohdistuu vain luonnolliselle henkilölle henkilökohtaisesti. Rikosoikeudellinen vastuu tulee tietosuojarikoksissa kyseeseen ainoastaan, kun teko on tahallinen, ellei myös tuottamuksesta ole säädetty rangaistusta (RL 5 §). Syytteen saa nostaa vain se, johon sillä on oikeus. Tieto- ja viestintärikosten syyteoikeudesta säädetään rikoslaissa.

Asianajajan ja avustajan salassapitovelvollisuuden myötä rikoslain 38.1 § salassapitorikoksesta tulee sovellettavaksi. Asianajotoimistossa työskentelevä asianajaja ei ole virkamies toisin kuin oikeusaputoimistossa työskentelevä asianajaja. Näin ollen tässä työssä ei ole oleellista tarkastella virkamiesrikoksia salassapidon ja tietoturvan kannalta. Muiden kuin virkamiesten tai näihin rinnastettavien henkilöiden salassapitorikos ei ole tuottamuksellisena rangaistava (RL 40.5). Näin ollen asianajajan ja avustajan salassapitorikos ei ole tuottamuksellisena rangaistava.

4.3 Muu menettely yleisessä tuomioistuimessa

Tietosuoja-asetuksessa säädetään rekisteröidyn oikeudesta vahingonkorvaukseen. Mikäli rekisteröidylle on aiheutunut vahinkoa tietosuoja-asetuksen loukkauksen perusteella, tulee tämän hakea vahingonkorvauksia yleisessä tuomioistuimessa (TS 82 artikla). Tietoturvaloukkauksen myötä myös yleisten vahingonkorvausperusteiden tai rikosoikeudellisen vahingonkorvausvastuun perusteella voi olla perusteita hakea vahingonkorvauksia. Vahingonkorvauksen perusteista säädetään vahingonkorvauslaissa (412/1974). Vahingonkorvausasia käsitellään yleisessä tuomioistuimessa joko rikosasian ohessa tai siviilikanteella. Riita-asian

[76] HE 9/2018, 124

oikeudenkäynnistä säädetään oikeudenkäymiskaaressa (683/2016), rikosasian ohessa käsiteltävä vahingonkorvausvaatimuksesta säädetään laissa oikeudenkäynnistä rikosasiassa (ROL). Vahingonkorvauslain mukaan vahingonkorvausvastuun perusteena on tahallisesti tai tuottamuksellisesti aiheutettu vahinko (VaHL (412/1974) 2:1 §). Korvattavasta vahingosta säädetään Vahingonkorvauslain 5 luvussa. Vahinkoa kärsineellä on näyttövelvollisuus aiheutuneesta vahingosta ja sen määrästä.[77]

Tietosuoja-asetuksen mukaisesti rekisteröity voi nostaa kanteen tietosuoja-asetuksen mukaisten oikeuksien toteuttamiseksi tai sen mukaisten oikeuksien rikkomisen oikeussuojaksi yleisessä tuomioistuimessa (TSA 79 artikla). Rekisteröity voi nostaa henkilötietojen käsittelyä koskevan asian riita-asiana velvoittamiskanteen tai vahvistuskanteen muodossa rekisterinpitäjää tai henkilötietojen käsittelijää vastaan yleisessä tuomioistuimessa.[78]

4.4 Asianajajaliiton kurinpitomenettely ja sanktiot

Asianajajaliiton valvovana mekanismina toimii riippumaton valvontalautakunta ja valvontayksikkö, joiden tehtävänä on valvoa asianajajia, julkisia oikeusavustajia sekä luvan saaneita oikeudenkäyntiavustajia (Asianajajalain 6 a §[79]). Valvonta-asian käsittelystä ja vireilletulosta säädetään asianajajalaissa. Asianajaja on vastuussa myös hänelle työskentelevien henkilöiden toimista suhteessa asianajajan velvollisuuksiin. Tämä tarkoittaa, että asianajaja joutuu vastaamaan valvontalautakunnalle myös palveluksessaan olevien henkilöiden toimista ja asianajajaliiton ohjeiden noudattamisesta sekä hyvän asianajajatavan noudattamisesta. Hyvä asianajajatapa määritellään laissa, Suomen asianajaliiton säännöissä säädetyn lisäksi tapaohjeista, muista liiton velvoittavista ohjeista, valvonta- ja kurinpitoasioissa annetuista ratkaisuista sekä asianajajakunnan hyväksytyistä käytännöistä.[80]

---

[77] Linna 2019, 78
[78] Lakivaliokunnan lausunto 5/2018, 18
[79] Laki asianajajista 716/2011
[80] Asianajajaliiton tapaohjeet 2019

Asianajajalain 7 §:n mukaan valvontalautakunnan on määrättävä asianajajalle kurinpidollinen seuraamus, mikäli valvonta-asian käsittelyssä ilmi tulleiden seikkojen johdosta hänen katsotaan menetelleen lain 5.1 §:n vastaisesti. Kyseissä pykälässä on määräys noudattaa hyvää asianajajatapaa:

> Asianajajan tulee rehellisesti ja tunnollisesti täyttää hänelle uskotut tehtävät sekä kaikessa toiminnassaan noudattaa hyvää asianajajatapaa. Kuluttajan kannalta sopimattomasta tai hyvän tavan vastaisesta menettelystä säädetään lisäksi kuluttajansuojalain (38/1978) 2 luvussa. (Asianajajalain 5.1 §)

Valvontalautakunnalla on valtuudet antaa kurinpidollinen seuraamus, joita ovat asianajajayhdistyksen jäsenyydestä erottaminen, seuraamusmaksun määrääminen, varoitus ja huomautus (asianajajalain 6 ja 7 §). Erotus seuraa epärehellisestä menettelystä tai tahallisesta toisen oikeuden loukkauksesta (asianajajalaki 7.2 §). Muusta menettelystä tulee 3 momentin mukaisesti varoitus tai huomautus. Toisaalta toistuvasta 2 tai 3 momentin mukaisesta menettelystä tai siihen liittyvistä raskauttavista seikoista johtuen voidaan erottaa tai määrätä seuraamusmaksu. Myös teosta, joka on omiaan alentamaan asianajajakunnan arvoa sovelletaan näitä säännöksiä. (Asianajajalaki 7 §)

Vaikutuksia kurinpitomenettelyllä on niin ammatinharjoittamisen kuin maineen kannalta. Valvontamenettelyn päätökset ovat julkisia ja ne kootaan julkiseen päiväkirjaan (Asianajajalaki 7 §). Julkaisu sisältää myös tiedon asian käsittelyn vaiheesta. Tieto seuraamuksesta poistetaan asianajajalain mukaisesti julkisesta päiväkirjasta kun

1) erottamisesta ja seuraamusmaksusta kymmenen vuoden kuluttua
2) varoituksesta kuuden vuoden kuluttua; ja
3) huomautuksesta ja siitä, että seuraamusta ei ole määrätty, kolmen vuoden kuluttua valvonta-asian ratkaisun antamisesta. Tietoa ei kuitenkaan poisteta, jos kyseisestä asianajajasta on päiväkirjassa sellainen seuraamusta tai palkkion alentamista tarkoittavaa suositusta koskeva uudempi tieto, jota ei 2 tai 3 momentin nojalla vielä voida poistaa. (asianajajalain 7 §)

Mikäli asianajaja erotetaan liitosta, seuraa erottamisesta kolmen vuoden jakso, jonka jälkeen hänet voidaan ottaa hakemuksesta uudelleen yhdistyksen jäseneksi. Seuraamusmaksun suuruudeksi määrätään asianajajalaissa vähintään 500 euroa ja enintään 15 000 euroa. Seuraamusmaksun suuruuteen vaikuttaa

asianajajan menettelyn moitittavuus, kokemus asianajotehtävistä sekä taloudelliset olot niin, että seuraamus on oikeudenmukaisessa suhteessa hänen menettelyynsä. Seuraamusmaksu suoritetaan asianajajayhdistykselle ja sillä katetaan valvontalautakunnan ja valvontayksikön toiminnasta aiheutuvia kustannuksia. Seuraamusmaksua ei määrätä, jos samaa rikkomusta koskeva asia on vireillä esitutkinnassa, syyteharkinnassa tai tuomioistuimessa rikosasiana taikka jos asianajaja on lainvoimaisesti tuomittu rangaistukseen kyseisestä rikkomuksesta. Seuraamus voidaan jättää määräämättä, jos asianajaja muulla tavalla hyvän asianajajatavan vastaisella menettelyllään vain vähäisessä määrin rikkoo asianajajan velvollisuuksia ja menettelyä on sen haitallisuuteen nähden pidettävä myös kokonaisuutena arvostellen vähäisenä. (asianajajalain 7 ja 7 a- h §)

4.5 Oikeussuojakeinon käytön kuluriski

Oikeussuojakeinojen käytöstä voi aiheutua rekisteröidylle kuluja niin asiamiehen käytöstä kuin oikeudenkäymiskuluista. Suomessa on eri mekanismeja, joilla oikeusturvakuluja voidaan korvata. Valtion oikeusapulain (OAL 257/2002) nojalla voidaan henkilölle antaa valtion varoista oikeusapua, johon kuuluu oikeudellinen neuvonta, tarpeellisia toimenpiteet sekä avustaminen tuomioistuimessa ja muussa viranomaisessa. Lisäksi hakija voidaan vapauttaa tarvittaessa tuomioistuinmaksuista. Oikeusapua myönnettäessä otetaan huomioon hakijan taloudellinen asema. Oikeusavun kattavuus määräytyy käyttövaran ja varallisuuden perusteella, oikeusapu kattaa normaalisti avustajan toimenpiteet enintään 80 tunnilta. Avustajan palkkion korvaamisen valtion varoista vahvistaa tuomioistuin. (OAL 1, 2, 4 ja 5 §)

Vakuutusyhtiöiden myöntämät, maksulliset oikeusturvavakuutukset korvaavat kuluja sopimusehtojen mukaan tuomioistuimissa. Vakuutusyhtiöillä on vakioehdot, joihin korvauksien myöntäminen perustuu. Oikeusturvavakuutuksista ei korvata kuluja, jotka ovat syntyneet lakimiesavun käyttämisestä esimerkiksi hallintoviranomaisissa tai hallinto-oikeudessa. Sen sijaan riita-asioissa sekä rikosasian asianomistajan kuluja asianajajan tai lakimiehen käytöstä korvataan vakuutuseh-

tojen mukaan. Vakuutusyhtiöiden oikeusturvavakuutuksissa on eroja korvauksien korvauspiirin ja vakuutusmäärän suhteen. Oikeusturvavakuutuksien yleisin kattavuus on 8500 euroa, jolloin omavastuun osuus vaihtelee 15-25 % välillä.[81]

4.5.1 Hallintotuomioistuinmenettely

Viranomaisen päätöksistä valitetaan ja haetaan muutosta hallintotuomioistuimissa. Tietosuojavaltuutetun toteutunut keskimääräinen käsittelyaika on ollut vuoden 2018 lopussa 38,4 päivää[82]. Tietosuojavaltuutetun käsittely on ilmoitusten ja rekisterinpitäjän toiminnasta valittamien osalta ilmaista. Tietosuojaviranomaisen päätöksestä valitetaan hallinto-oikeuteen. Keskimääräinen toteutunut käsittelyaika hallinto-oikeudessa on vuonna 2018 ollut 9,6 kuukautta[83]. Korkeimmassa hallinto-oikeudessa toteutunut keskimääräinen käsittelyaika muissa kuin ulkomaalaisasioissa on vuonna 2018 ollut 11,4 kuukautta[84] . Hallinto-oikeuden päätöksen yhteydessä perittävä oikeudenkäyntimaksu on vuonna 2020 suuruudeltaan 260 euroa. Maksua ei peritä, kun hallinto-oikeus muuttaa valituksenalaisen päätöksen valittajan eduksi. Oikeusapua hallintoasioissa voidaan myöntää oikeusapulain nojalla niin avustajan kustannuksiin kuin oikeudellisen neuvonnan muodossa. Vakuutusyhtiöt eivät korvaa hallintotuomioistuinkäsittelystä aiheutuneita asiamies- tai tuomioistuinkuluja.[85]

4.5.2 Rikosoikeudellinen menettely

Oikeusapua voidaan myöntää hakijalle oikeusapulain nojalla. Vakuutukset kattavat asianomistajan kuluja vakuutusehtojen mukaan rikosasioissa. Rikosoikeudellisen menettelyn kestoa arvioidessa rekisteröidyn kannalta tulee ottaa huomioon myös esitutkintavaiheen ja syyteharkinnan kesto. Tavoitteellinen palvelutaso rikoslakirikosten selvitystasoksi (pl. liikennerikokset) on vähintään 48,5 % vuodelle

---

[81] Fine 2018, 4-5
[82] Tietosuojavaltuutetun toimiston toimintakertomus 2018, 8
[83] Budjettiesitys, 177
[84] Budjettiesitys, 174
[85] Tuomioistuinten maksut, 2019. Fine 2018, 4

2020, tutkinta-aika keskimäärin 135 vrk. Toteutunut syyteharkinta-aika on ollut vuonna 2018 keskimäärin 1,7 kuukautta, samaan aikaan yli 6 kk syyteharkinnassa on ollut avoinna 2 231 ja yli vuoden 327 kpl rikosasiaa.[86]

Keskimääräinen toteutunut käsittelyaika rikosasioiden käräjäoikeusvaiheessa on vuonna 2018 ollut noin 4,4 kuukautta. Hovioikeuksien kaikkien asioiden keskimääräinen toteutunut käsittelyaika on vuonna 2018 ollut noin 5,6 kuukautta. Oikeusavun määrärahasta on arvioitu vuonna 2020 käytettäväksi yksityisille oikeusavustajille 200 000 euroa valtiotasolla asianomistajan avustamiseen. Yleisen tuomioistuimen käräjäoikeusvaiheen oikeudenkäyntimaksu rikosasian osalta on 260 euroa. Oikeudenkäyntimaksua ei peritä, kun syyttäjä ajaa syytettä. [87]

4.5.3 Muu yleisen tuomioistuimen käsittely

Vahingonkorvausasian ajaminen siviilikanteena käräjäoikeudessa kuuluu oikeusturvavakuutuksen katettavaksi. Siviilikanteen nostamisen yhteydessä on syytä nostaa esille suuri riski vastapuolen oikeudenkäyntikuluista maksettavaksi lankeamisesta asian häviämisen yhteydessä, niitä oikeusturvavakuutukset eivät nykyisin yleensä kata. Oikeusapua ei saa riita-asioissa oikeusapulain nojalla, mikäli asia on hakijalle vähämerkityksinen. Arvioinnin tekee oikeusaputoimisto oikeusapulain nojalla.[88]

Keskimääräinen toteutunut käsittelyaika ei-summaaristen riita-asioiden käräjäoikeusvaiheessa on noin 9,8 kuukautta (toteutunut vuonna 2018). Hovioikeuksien kaikkien asioiden keskimääräinen käsittelyaika on vuonna 2018 ollut noin 5,6 kuukautta. Korkeimman oikeuden keskimääräinen käsittelyaika on ollut valituslupa-asioissa 4,3 kk ja asiaratkaisuissa 18,7 kuukautta (vuonna 2018). Riita-asian käsittelystä perittävä oikeudenkäyntimaksu on 510 euroa.[89]

---

[86] Budjettiehdotus 187
[87] Budjettiehdotus 177-186
[88] Fine 2018, 4-5
[89] Budjettiehdotus, 177. Tuomioistuinten maksut, 2019.

4.5.4 Valvontalautakunnan menettely

Valvontalautakunta on ilmoittanut vuosikertomuksessaan keskimääräiseksi valvonta-asioiden käsittelyajaksi 7 kk 91 päivää.[90] Valvontalautakunnan menettelystä aiheutuneisiin asiamieskuluihin ei saa oikeusturvavakuutuksen nojalla korvauksia. Valtion oikeusapua ei myönnetä kanteluun, oikeudellista neuvontaa on saatavilla oikeusaputoimistoissa. Tässä yhteydessä on syytä huomioida, että osapuolina valvontamenettelyssä ovat asian alkuun saattamisen jälkeen valvontalautakunta sekä asianajaja, josta on valitettu. Kantelijalla ei ole muutoksenhakuoikeutta valvontapäätöksistä. Ylimääräisenä muutoksenhakukeinona kantelija voi tehdä kantelun valvontalautakunnan ratkaisusta valtioneuvoston oikeuskanslerille. Valvontalautakunnan menettelystä ei aiheudu oikeudenkäyntimaksuja kantelijalle.

[90] Valvontakertomus 2018, 65

5 YHTEENVETO JA POHDINTA

Rekisteröidyllä on tietoturvaloukkaustilanteessa käytössään monia eri oikeussuojakeinoja. Riippuen siitä, mitä lakisääteistä oikeutta on loukattu, valikoituu eri oikeussuojakeino käytettäväksi. Työssä käsiteltiin keskeisiä rekisteröidyn oikeussuojakeinoja rekisterinpitäjää kohtaan. Ylimääräiset muutoksenhakukeinot jätettiin aiheen ulkopuolelle. Rekisteröity saa tietoja henkilötietojen käsittelystä rekisterinpitäjältä sekä tietosuojavaltuutetun toimistolta.

Rekisteröidyn oikeusturvakeinot ovat valitus tai ilmoitus tietosuojaviranomaiselle, vahingonkorvaus-, vahvistus- tai velvoittamiskanne yleisessä tuomioistuimessa, rikosilmoitus sekä valvontamenettelyn alulle saattaminen asianajajaliiton valvontalautakunnassa. Oikeussuojakeinon valinta tulee tehdä arvioimalla sitä, onko mahdollisesti tapahtunut rikos, onko henkilötietojen luokkauksesta aiheutunut vahinkoa? Mikäli ei ole aiheutunut vahinkoa vahingonkorvauslain mukaisesti eikä rikosta tapahtunut, tulee tietosuojaviranomaisen johdolla tehtävä menettely kyseeseen. Tietosuojaviranomaisen menettely ei korvaa rekisteröidylle aiheutunutta vahinkoa vaan sen tarkoitus on enemmänkin ohjata rekisterinpitäjää toimimaan jatkossa asianmukaisesti.

Työn aiheen rajauksesta johtuen rikosoikeudellisen tarkastelun ulkopuolelle jätettiin kolmannen osapuolen vastuulle jäävät rikokset kuten hakkerointi, viestintärauhan rikkominen ja viestintäsalaisuuden rikkominen. Myöskään asianajotoimiston sisällä tapahtuvaa urkintaa ei sinällään käsitelty, se koskee rekisterinpitäjää vain henkilötietojen käytön ja lokitietojen valvonnan näkökulmasta.

Työssä tärkein havainto oli, että tietoturvaloukkauksesta ei aiheudu kovinkaan helposti sanktioita rekisterinpitäjälle. Tietoturvan vaadittavasta tasosta etsittiin tietoa monipuolisesti mm. tietosuoja-asetuksesta mutta kaikkein merkittävimmäksi rekisterinpitäjän vastuun kannalta myös tietoturvan suhteen osoittautui osoitusvelvollisuuden täyttäminen. Käytännössä rekisterinpitäjän tulee osata vastata pyyntöihin asianmukaisesti sellaisilla termeillä ja menettelyillä, jotka hallintoviranomainen hyväksyy ja ymmärtää. Ainakin tällä hetkellä tietosuojaviranomainen on valinnut linjakseen antaa huomautuksia tarkoituksenaan ohjeistaa

rekisterinpitäjiä ja henkilötietojen käsittelijöitä tietosuoja-asetuksen noudattamisesta. Tietosuojaviranomainen on julkaissut muun muassa ratkaisun, jossa se antoi huomautuksen POP Pankille puutteellisesta tiedotuksesta tietoturvaloukkauksen kohteeksi joutuneille (60/171/2020)[91]. Huomautusasiassa oli kyse siitä, että rekisterinpitäjä oli julkaissut julkisen tietoturvaloukkausilmoituksen facebook -sivullaan, jonka sisällöstä saattoi saada virheellisesti käsityksen, että rekisterinpitäjä olisi ollut yhteydessä kaikkiin loukkauksen kohteeksi joutuneisiin henkilökohtaisesti. Tietosuojavaltuutettu on ratkaisussaan 2694/171/19 painottanut rekisterinpitäjän dokumentointivelvollisuutta tietoturvaloukkauksen seikkojen, vaikutusten ja korjaavien toimien suhteen. Dokumentoinnin avulla valvontaviranomainen voi tarkistaa, että tietosuoja-asetuksen 33 artiklan 5 kohtaa on noudatettu.[92]

Prosesseista yleisessä tuomioistuimessa kantajan aloitteesta käytävä prosessi on kaikista kallein ja suuririskisin. Kantajalle muodostuu asiamieskuluja, tuomioistuinkulut sekä riski vastapuolen kuluista, mikäli vahingonkorvauskanne hylätään. Tietosuojaviranomaisen johdolla tehdystä menettelystä ei tule rekisteröidylle kuluja. Rikosoikeudellinen menettely syyttäjävetoisena on asianomistajan kannalta kuluton, mutta toisaalta asiamieskuluja voi tulla. Asianajajaliiton valvontamenettely on valittajalle kuluton. Asianajajaliiton valvontalautakunta on työn aihepiiriin liittyen antanut yhden huomautuksen luvan saaneelle oikeudenkäyntiavustajalle. Asiassa oli kyse salassapitovelvollisuuden rikkomisesta lähettämällä vahingossa kolmannelle osapuolelle sähköpostin liitteenä kuolinpesätoimeksiantoon liittyviä asiakirjoja. Myös asiakkaansa salaiset yhteystiedot pesänjakajan hakemukseen kirjannut ja käräjäoikeuteen toimittanut asianajaja selvisi huomautuksella ja hänen katsottiin rikkoneen huolellisuusvelvoitetta.[93]

Luotettavuutta arvioidessa on arvioitava lähteiden valintaa ja rajausta. Työhön on valittu pääasiallisiksi lähteiksi lakitekstejä sekä viranomaislähteitä. Lähteet ovat luotettavia alkuperäislähteitä. Lähteiden ylimalkaista tulkintaa on pyritty välttämään, työssä on pääosin selvitetty lakitekstejä viranomaislähteiden avulla. Työ

[91] Finlex
[92] Tietosuoja.fi 2020
[93] valvontalautakunta.fi 2018

onnistui odotetusti. Vaikeinta työtä tehdessä oli aiheen rajaus sekä eri oikeussuojakeinojen suhteiden ymmärtäminen. Hyväksi punaiseksi langaksi muodostui se, että prosessit esitettiin erikseen niin, että jokaisen oikeussuojaprosessin takana on eri toimivaltainen viranomainen tai valvontamekanismi. Lisätutkimuksena voisi tutkia osoitusvelvollisuuden täyttymistä tietoturvallisuuden osalta. Osoitusvelvollisuuden kannalta olisi mielenkiintoista saada vastauksia siihen, mitkä osoitusvelvollisuuden täyttämisen tavat vähentävät rekisterinpitäjän vastuuta esimerkiksi palvelimen kaatuessa ja levittäessä tietoja ulkopuolisille. Tämä vaatisi laajaa IT-osaamista sekä oikeuskäytäntöä lakitekstien tulkinnan lisäksi.

LÄHTEET

Asianajajaliitto: Oikeusministeriön päätös yleisen asianajajayhdistyksen sääntöjen vahvistamiseksi (Suomen asianajajaliiton säännöt, muut. viim. 2.4.2019/439. https://asianajajaliitto.fi/asianajajaksi/suorita-asianajajatutkinto/asianajotoimintaa-koskevia-saadoksia-ja-ohjeita/

Asianajajaliitto: Tapaohjeet. Asianajajaliiton tapaohjeet. 2012. Asianajajaliiton valtuuskunta. Luettu 13.10.2019. https://asianajajaliitto.fi/tapaohjeet/

Asianajajaliitto: Tietoturvaopas. 12.12.2019. Asianajajaliiton hallitus. https://asianajajaliitto.fi/asianajajaksi/suorita-asianajajatutkinto/asianajotoimintaa-koskevia-saadoksia-ja-ohjeita/

Asianajajaliitto: Valvontakertomus 2018. 2019. Valvontalautakunta. Luettu 1.4.2020 https://www.valvontalautakunta.fi/valvontalautakunta/valvontakertomus Budjettiesitys 2020. 2019. Valtion talousarvio, Valtioneuvosto. Luettu 1.3.2020, https://valtioneuvosto.fi/budjetti-2020

"Esimerkkejä henkilötietojen tietoturvaloukkauksista ja siitä, kenelle niistä ilmoitetaan. Tietosuojatyöryhmä. Luettu 13.2.2020 https://tietosuoja.fi/documents/6927448/8214536/Esimerkkej%C3%A4+tietoturvaloukkauksista/754c16aa-152e-4f15-a458-d1579c5ea4b2/Esimerkkej%C3%A4+tietoturvaloukkauksista.pdf"

Fine: Perustietoa oikeusturvavakuutuksista. 2018. Luettu 2.2.2020. https://www.fine.fi/julkaisut/julkaisu/perustietoa-oikeusturvavakuutuksista.html

Guide to holistic cyber security. 2019. F-Secure.

Hirvonen, A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Helsinki: Yleisen oikeustieteen julkaisuja 17. https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Ilmoitus tietoturvaloukkauksesta. Tietosuojavaltuutetun toimisto. Luettu 16.3.2020 https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

Koillinen, M. 2016. Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. Defensor Legis – lehti 4/2016, 570.

Korpisaari, P. & Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Alma Talent verkkopalvelu. Vaatii käyttöoikeuden https://verkkokirjahylly-almatalent-fi.libproxy.tuni.fi/teos/BAXBBXATHBBED

Lainkirjoittajan opas. 5.9.2013 Oikeusministeriö. Luettu 5.9.2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/76493/lainkirjoittajan_opas_low_20130904.pdf

Linna, T. 2019. Prosessioikeuden oppikirja. Alma Talent. Vaatii käyttöoikeuden. https://fokus-almatalent-fi.libproxy.tuni.fi/teos/BAXBBXATJFCBJ#kohta:PROSESSIOIKEUS/piste:td

Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski". 2017. Tietosuojatyöryhmä. https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9debe21bdd2e0a63/Vaikutustenarviointi+fi.pdf

Oikeuskanslerinvirasto: Asianajajien valvonta. Luettu 2.3.2020. https://www.okv.fi/fi/oikeuskansleri/tehtavat_ja_toiminta/asianajajien-valvonta/
Oikeusturvan toteutuminen. Oikeusministeriö. Luettu 3.5.2020 https://oikeusministerio.fi/oikeusturvan-toteutuminen

Osoita noudattavasi tietosuojasäännöksiä. Tietosuojavaltuutetun toimisto. Luettu 12.3.2020. https://tietosuoja.fi/osoitusvelvollisuus

Pitkänen, P. 2016. Tulevan tietosuojalain rikkomisesta voi tulla kymmenien miljoonien sakot: "Tarkoitus ei ole kerätä rahaa". Iltasanomat. Luettu 10.1.2020. https://www.is.fi/digitoday/art-2000001906519.html

POP Pankille huomautus puutteellisesta tiedotuksesta tietoturvaloukkauksen kohteeksi joutuneille. 15.1.2020. Tietosuojavaltuutetun toimisto. Luettu 15.4.2020. https://tietosuoja.fi/artikkeli/-/asset_publisher/pop-pankille-huomautus-puutteellisesta-tiedotuksesta-tietoturvaloukkauksen-kohteeksi-joutuneille

Rekisterinpitäjän velvollisuuksien toteuttaminen. Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet.. 2017. Valtiovarainministeriö https://vm.fi/documents/10623/4914009/Rekisterinpit%C3%A4j%C3%A4n+velvollisuuksien+toteuttaminen/ccb2542e-7699-48fa-8d9b-9c6fa4a87640/Rekisterinpit%C3%A4j%C3%A4n+velvollisuuksien+toteuttaminen.pdf

Theseus - ammattikorkeakoulujen opinnäytetyöt ja julkaisut verkossa. Luettu 4.5.2020. https://www.theseus.fi/

Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. 2019. Tietosuojavaltuutetun toimisto. Luettu 4.5.2020 https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimistolle on ilmoitettu jo 2700 henkilötietojen tietoturvaloukkausta. 22.2.2019. Tietosuojavaltuutetun toimisto. Luettu 8.11.2019. https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-toimistolle-on-ilmoitettu-jo-2700-henkilotietojen-tietoturvaloukkausta

Tietosuojavaltuutetun toimiston toimintakertomus 2018. 2019. https://tietosuoja.fi/documents/6927448/10717840/Toimintakertomus+2018/92fffcd7-1e06-2c5e-003e-7fa53aaa72f2/Toimintakertomus+2018.pdf

Tietoturvaloukkaukset. Tietosuojavaltuutetun toimisto. Luettu 20.4.2020. https://tietosuoja.fi/tietoturvaloukkaukset

Tietoturvaohje B 5.1. 2020. Asianajotoimintaa koskevia säädöksiä ja ohjeita. Luettu 2.2.2020. https://asianajajaliitto.fi/asianajajaksi/suorita-asianajajatutkinto/asianajotoimintaa-koskevia-saadoksia-ja-ohjeita/

Tuomioistuinten maksut. 1.1.2019. Oikeusministeriö. Luettu 1.3.2020. https://oikeus.fi/tuomioistuimet/hallintooikeudet/fi/index/maksut/muuttuomioistuimet.html

Vahti: Tietoturvapoikkeamien hallinta. 2017. Valtiovarainministeriön julkaisuja 8/2017. Luettu 5.3.2020. http://urn.fi/URN:ISBN: 978-952-251-930-6

Valiokunnan lausunto 5/2018vp. 24.5.2018. Lakivaliokunta. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/LaVL_5+2018.pdf

Valvontaratkaisujen hakemisto. Asianajajaliitto. Luettu 2020. https://www.valvontalautakunta.fi/valvontalautakunta/valvontaratkaisuja

Viestintäviraston tilinpäätös vuodelta 2018. 2019. Viestintävirasto. Luettu 3.3.2020. https://www.traficom.fi/sites/default/files/media/file/Viestintäviraston-tilinpäätös-2018.pdf

Virallisen syytteen alaiset rikokset ja asianomistajarikokset. Poliisi. https://www.poliisi.fi/rikokset/virallisen_syytteen_alaiset_rikokset_ja_asianomistajarikokset

Vuosikertomus 2018. 2019. Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/toimintakertomus-2018

LIITTEET

Liite 1. Asianajaliiton tietoturvaohje B 5.1 2020

Asianajajan on huolehdittava, että

1. Hänen oma ja toimiston henkilökunnan tietoturvaa koskeva osaaminen on riittävän korkealla tasolla siten, että tätä ohjetta ja tietoturvaopasta (B 5.2) voidaan soveltaa toiminnan järjestämisessä. Vähintään 10 työntekijän asianajotoimiston on järjestettävä ulkoinen tietoturva-auditointi säännöllisin väliajoin.
2. Asianajotoimistoon tai asianajotoimintaan ei toteuteta sellaisia tarkastuksia tai tietopyyntöjä, joihin sisältyy asianajotoiminnan järjestämistä, asiakkuuksia tai toimeksiantoja koskevien tietojen keräämistä tai luovuttamista asiakkaille, palveluntarjoajille tai muille ulkopuolisille osapuolille. (16.1.2020, voimaan 1.2.2020)
3. Käytössä olevat fyysiset toimitilat ovat lukitut ja muutoinkin suojatut. Kaikki asianajajasalaisuuden piirin kuuluva aineisto, riippumatta siitä, miten tieto on tallennettu tai säilytetty, on suojattu.
4. Asianajotoiminnassa käytettävien laitteiden ja välineiden tiedot on salattu (kryptattu). Näitä laitteita ja välineitä ei saa antaa ulkopuolisten käyttöön. Asianajosalaisuuden säilyttämiseksi tulee välttää vieraiden laitteiden käyttöä tai niiden kytkemistä omiin laitteisiin. Laitteiden elinkaarista on huolehdittava siten, että laitteet, joihin ei enää tarjota päivityksiä, poistetaan käytöstä ja vaihdetaan uusiin.
5. Toimiston tai asianajajan laitteissaan käyttämät langattomat verkot on suojattu. Toimiston vierailijoilla ei tule olla pääsyä toimiston sisäiseen verkkoon (vieraille on järjestetty esimerkiksi oma langaton verkko). Käytettäessä julkisia verkkoja on käytettävä salattua yhteyttä (vpn tai vastaava).
6. Käytettävät salasanat ovat riittävän monimutkaisia, ne vaihdetaan tarpeeksi usein ja huolehditaan, etteivät muut pääse niihin käsiksi. Lisätunnistautumismenetelmiä käytetään mahdollisuuksien mukaan korkeamman tietoturvatason saavuttamiseksi.
7. Tietoturvaohjelmistot ja palomuuri ovat kunnossa. Laitteiden, käyttöjärjestelmien, ohjelmien ja sovellusten päivitykset asennetaan ilman aiheetonta viivästystä.
8. Asiakirjoihin tulee olla pääsy vain niillä henkilöillä, jotka tarvitsevat tai

saattavat tarvita salassa pidettäviä tietoja tai ainakin pääsyä kyseisiin tiedostoihin työtehtäviensä hoitamiseksi.

9. Varmuuskopiointi tehdään säännöllisesti. Varmuuskopioita sisältävät laitteet ja mediat on salattu ja huolellisesti säilytetty. Varmuuskopioiden säännöllisestä testaamisesta huolehditaan.

10.Kaikkien ulkopuolisten palveluntarjoajien kanssa tehtävät sopimukset täyttävät tietoturvavaatimukset, ts. sisältävät etenkin salassapitoa koskevat ehdot (erityisesti ulkoistetut it-palvelut, toimitiloihin pääsevät tahot).

11.Kaikki sähköpostilla tai muulla sähköisellä tavalla lähetettävä aineisto on tarvittaessa salattu. Asianajajan on huolehdittava aineiston salaamisesta, jos sisältö on erityisen sensitiivistä tai asiakas edellyttää salattua liikennettä, sekä tarvittaessa ohjeistettava asiakastaan toimittamaan aineisto suojatulla menetelmällä.

12.Asiakirjat ja muu aineisto tallennetaan, säilytetään, arkistoidaan ja tuhotaan tietoturvallisella tavalla.

13.Kaikki tietoa sisältävät laitteet poistetaan käytöstä ja tyhjennetään tietoturvallisella tavalla (tietokoneet, mobiililaitteet, tallennusvälineet jne). Sama koskee käytössä olevia tallennus- ja verkkopalveluita.

14.Toiminnan jatkuvuudesta on huolehdittu siten, että toimiston jatkuvuuden kannalta tarvittavat tiedot on kootusti dokumentoitu ja tämä dokumentointi on jatkuvuudesta huolehtivien tahojen saatavilla