Opinnäytetyö (AMK)

Liiketalouden koulutusohjelma

Juridiikka

2018

Dina Ahonen

EUROOPAN UNIONIN YLEINEN TIETOSUOJA-ASETUS

– Vaikutus vakuutusyhtiön korvausorganisaation toimintaan

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalouden koulutusohjelma | Juridiikka

2018 | 36 sivua

Dina Ahonen

UUSI EUROOPAN UNIONIN YLEINEN TIETOSUOJA-ASETUS

- Vaikutus vakuutusyhtiön korvausorganisaation toimintaan

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsitellessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Euroopan parlamentti ja neuvosto ovat säätäneet yleisen tietosuoja-asetuksen 2016/679 (EU). Yleinen tietosuoja-asetus tulee suoraan sovellettavaksi Euroopan unionin jäsenvaltioissa 25.5.2018.

Uusi asetus vaatii nykyisen lainsäädännön muokkaamista ja täydentämistä. Tämän vuoksi oikeusministeriön asettama työryhmä ehdottaa, että Suomen lainsäädäntöön säädettäisiin uusi henkilötietojen suojaa koskeva yleislaki, jota kutsuttaisiin nimellä tietosuojalaki. 1.3.2018 annettiin hallituksen esitys uudesta tietosuojalaista. Kyseessä olisi yleislaki, jota sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa. Lain on tarkoitus tulla voimaan 25.5.2018, eli samana päivänä, jolloin Euroopan unionin tietosuoja-asetusta aletaan soveltaa jäsenvaltioissa.

Tämän opinnäytetyön aiheena on selvittää erot henkilötietojen suojassa vanhan ja uuden lainsäädännön välillä. Opinnäytetyön tarkoituksena on kartoittaa näiden lakien ja asetusten erot sekä ylipäätään selventää, miten henkilötietoja on suojattu ennen muutosta ja miten niitä tullaan suojaamaan jatkossa. Tarkoituksena on myös selvittää, miten muutos vaikuttaa vakuutusyhtiön korvausorganisaatioon ja sen käytäntöihin henkilötietojen suojaa koskien.

Opinnäytetyön aihe ja tavoitteet syntyivät tekijän oman henkilökohtaisen mielenkiinnon sekä omiin työtehtäviin liittyvän kiinnostuksen perusteella. Opinnäytetyö perustuu vahvasti teoriaan ja työ on tehty täysin teoreettisena tutkielmana. Lähdeaineisto koostuu pääasiassa lainsäädännöstä ja sitä tukevista internetlähteistä.

Opinnäytetyössä todetaan, että uusi lainsäädäntö on tarpeen muuttuneen maailman vuoksi, sillä digitalisaatio ja globalisaatio ovat muuttaneet henkilötietojen käsittelyä. Lainsäädännön mukauttaminen ajantasaiseksi edesauttaa niin rekisteröityä kuin myös rekisterinpitäjää, joka käsittelee tai pitää hallussaan henkilötietoja.

ASIASANAT:

tietosuoja, henkilötiedot, henkilötietolaki, EU-asetus, asetus, lainsäädäntö

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme of Business Administration | Jurisprudence

2018 | 36 pages

Dina Ahonen

GENERAL DATA PROTECTION REGULATION OF THE EUROPEAN UNION

- Effect to Operation of a Claims Organization of Insurance Company

The purpose of the personal data legislation is to carry out the protection of private life and other protection of privacy protective fundamental rights when handling personal data and to promote developing and following the good data processing practice. The European Parliament and the Council of Europe have prescribed the General Data Protection Regulation EU 2016/679. The General Data Protection Regulation will become applicable in every member state of the European Union by 25 May 2018.

The new regulation requires a change and complement to the current legislation. Therefore, a work group of the Ministry of Justice proposes that a new common law of protection of personal data would be prescribed in the Finnish legislation and be called as privacy law. On 1 March 2018 there was given a proposal by the Finnish Board of Directors about the new privacy law. The new law would be a common law that would be adapted alongside the new regulation. The European Union's regulation will apply 25 May 2018 in the member states of the European Union. On the same day, the Finnish privacy law will also be taken to effect.

The goal of this thesis is to clarify the differences in the personal data protection between the previous and the new legislation. The purpose is to chart the differences in these legislations and regulations and in the first place to clarify how personal data has been protected prior to this change and how it will be protected in the future. In addition, the thesis clarifies how the change will affect an insurance company's claims organization and the practices about the personal data handling.

The subject and the targets are based on author's personal interest and the interest in duty at work. The thesis relies strongly on theory and the text is fully a theoretical study. The source materials are mainly about legislation and web based sources that support the legislation.

The thesis states that the new legislation is necessary since the world has changed greatly. Digitalization and globalization have been changing the way that personal data is handled. The adaptation of the legislation to real-time will help the consumer and also the data controller that handles or possess the personal data.

KEYWORDS:

privacy protection, personal data, personal data legislation, regulation of EU, regulation, legislation

SISÄLTÖ

KUVIO

LYHENTEET

EU	Euroopan Unioni
HE	Hallituksen esitys
HeTiL	Henkilötietolaki 523/1999
GDPR	General Data Protection Regulation (EU:n yleinen tietosuoja- asetus)

1 JOHDANTO

Tämän opinnäytetyön aiheena on uusi Euroopan unionin yleinen tietosuoja-asetus 2016/679 (EU). Tarkoituksena on verrata nykyisen lainsäädännön ja uuden lainsäädännön eroja sekä sitä, miten tämä henkilötietoihin liittyvä sääntelyn muutos vaikuttaa vakuutusyhtiön korvausorganisaation toimintaan. Miten henkilötietoja täytyy jatkossa käsitellä ja mitä velvollisuuksia rekisterinpitäjälle muodostuu? Tavoitteena on, että tämän opinnäytetyön lukemisen jälkeen sekä rekisterinpitäjä että rekisteröity ymmärtää, miten henkilötietoja pitää jatkossa käsitellä ja mitä oikeuksia rekisteröidyllä on. Lisäksi on tärkeää ymmärtää, että vaikka uudistus vaatii paljon rekisterinpitäjien valmistautumista muutokseen, on sääntelyn yhtenäistäminen ja uudistaminen lopulta vain hyvä asia.

Opinnäytetyö on tehty teoreettisena tutkielmana. Lähdemateriaalit koostuvat pääasiassa lainsäädännöstä, hallituksen esityksestä sekä näitä tukevasta verkkopohjaisesta materiaalista. Kirjallisuudesta ei löytynyt yhtä ajankohtaista ja päivitettyä tietoa kuin verkkolähteistä. Näin ajankohtaisesta aiheesta uusimmat tiedot löytyvät verkosta, joten lähteet ovat lähes ainoastaan internet-lähteitä. Hallituksen esitys annettiin vasta 1.3.2018, eli loppuvaiheessa opinnäytetyöni tekoa, joten se vaikutti jonkun verran opinnäytetyön muodostumiseen. Työ on tehty niillä tiedoilla, jotka olivat saatavilla työn tekovaiheessa.

Kiinnostuin aiheesta, koska tämä aihe on ollut puheenaiheena töissäni vakuutusyhtiössä jo pidemmän aikaa. Lisäksi koin, että aihe on juuri nyt niin ajankohtainen, että minun on pakko tutkia sitä lisää. Uudistus vaikuttaa työhöni, joten opinnäytetyön kirjoittaminen kyseisestä aiheesta auttaa minua varmasti myös työssäni. Olen aiemminkin joutunut noudattamaan tarkkoja sääntöjä henkilötietojen käsittelyyn liittyen. Jatkossa on kuitenkin erittäin tärkeää noudattaa uusia yhtenäisiä sääntöjä entistäkin tarkemmin.

Opinnäytetyöni alkaa nykyisen henkilötietojen suojaa koskevan lainsäädännön läpikäymisellä, sillä ensin on hyvä tietää, minkälaista sääntelyä ennen uudistusta on pitänyt noudattaa. Sen jälkeen käyn läpi Euroopan unionin yleistä tietosuoja-asetusta sekä hallituksen esitystä uudesta tietosuojalaista. Lopuksi käyn läpi henkilötietojen suojaa koskevan lainsäädännön uudistuksien vaikutusta vakuutusyhtiön korvausorganisaation toimintaan.

2 HENKILÖTIETOJEN SUOJAA KOSKEVAN SÄÄNTELYN NYKYTILA

2.1 Yleistä

Suomen perustuslain 2 luvun 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Tätä sääntelee Suomessa pääasiassa henkilötietolaki (HeTiL), joka on ollut voimassa 22.4.1999 alkaen. Laki kumoaa aiemmin voimassa olleen henkilörekisterilain (471/1987).

HeTiL:n 1 luvun 1 §:n mukaan tämän lain tarkoituksena on ”toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.” Lakia sovelletaan henkilötietojen käsittelyyn ja se koskee viranomaisten, yritysten, järjestöjen, muiden yhteisöjen ja yksityisten henkilöiden toimintaa.[1]

Henkilötietojen suojaan läheisesti liittyviä perusoikeuksia ovat yksityiselämän suojan lisäksi oikeus kunniaan ja yhdenvertaiseen kohteluun, oikeus henkilökohtaiseen koskemattomuuteen, oikeus ihmisarvoiseen kohteluun, oikeus turvallisuuteen sekä yhdenvertaisuuteen, oikeus vaikuttaa itseään koskeviin asioihin, uskonnon ja omatunnon vapaus, sananvapaus sekä julkisuus.[2]

Euroopan parlamentti ja neuvosto ovat säätäneet 2016 keväällä yleisen tietosuoja-asetuksen 2016/679 (EU). Tämä asetus kumoaa Euroopan unionin (EU:n) henkilötietodirektiivin 95/46/EY, joka on täytäntöönpantu Suomessa henkilötietolailla (523/1999). Yleistä tietosuoja-asetusta tullaan soveltamaan suoraan EU:n jäsenvaltioissa 25.5.2018. Jäsenvaltioiden lainsäätäjille jää kuitenkin jonkin verran säännöksiä täsmentävää ja täydentävää liikkumavaraa.[3] Ensin on kuitenkin hyvä tutustua Suomen nykyiseen lainsäädäntöön henkilötietojen osalta sekä niiden tietosuojaan liittyen.

[1] Tietosuojavaltuutetun toimisto 2017a, 3
[2] HE 9/2018
[3] Valtioneuvosto 2017, 13

2.2 Henkilötietolain määritelmät

Nykyisen henkilötietolain (523/1999) mukaan henkilötiedolla tarkoitetaan kaikenlaista luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. Näiden tietojen käsittelyllä taas tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.

Henkilörekisteri on henkilötietoja sisältävä tietojoukko, jossa tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia.[4] Rekisterinpitäjä vastaa siitä, että näitä tietoja käsitellään lain vaatimusten mukaisesti.[5] HeTiL:n 1 luvun 3 §:n mukaan ”rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty.” Onkin tärkeää, että rekisterinpitäjä selvittää miksi kerää henkilötietoja, ja että tietojen käsittely on lainmukaista.

HeTiL:n 2 luvun 5 §:n huolellisuusvelvoitteen mukaan ”rekisterinpitäjän tulee käsitellä näitä tietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta.” Saman luvun kuudennen pykälän mukaan henkilötietojen käsittelyn on oltava asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietoja saa käsitellä ainoastaan seuraavissa henkilötietolain 2 luvun 8 §:ssä mainituissa tilanteissa:

1. rekisteröidyn yksiselitteisesti antamalla suostumuksella;
2. rekisteröidyn toimeksiannon perusteella tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;

[4] Tietosuojavaltuutetun toimisto 2017a, 3
[5] Tietosuojavaltuutetun toimisto 2017a, 4

3. jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi;

4. jos käsittelystä on säädetty laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta;

5. jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan;

6. jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista;

7. jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita näihin verrattavia tehtäviä varten;

8. jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi; tai

9. jos tietosuojalautakunta on antanut käsittelyyn 43 §:n 1 momentissa tarkoitetun luvan.

Luettelon yhdeksännellä kohdalla tarkoitetaan HeTiL:n 43 §:n 1 momentin mukaan tietosuojalautakunnan antamaa lupaa henkilötietojen käsittelyyn, jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi jossakin muussa kuin yksittäistapauksessa taikka yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan. Henkilötietolain vastaisesta menettelystä voi olla seuraamuksena rikosoikeudellinen rangaistus tai vahingonkorvausvastuu.[6]

[6] Tietosuojavaltuutetun toimisto 2017a, 9

2.3 Arkaluontoisten tietojen sekä henkilötunnuksen käsittely

HeTiL:n 2 luvun 11 §:n mukaan arkaluontoisten henkilötietojen käsittely on kielletty. Tällaisia henkilötietoja ovat seuraavassa listassa olevat kohdat, jotka kuvaavat tai on tarkoitettu kuvaamaan:

1. henkilön rotua tai etnistä alkuperää;
2. henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
3. rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
4. henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
5. henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
6. henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Näihinkin kohtiin on kuitenkin olemassa poikkeuksia. Opinnäytetyön aihetta lähellä on erityisesti HeTiL:n 3 luvun 12 §:ssä mainittu kohta 11, jonka mukaan pykälässä 11 säädetyt kohdat eivät estä vakuutuslaitosta käsittelemästä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista taikka sellaisia tietoja vakuutetun, korvauksenhakijan tai vahingon aiheuttajan rikollisesta teosta, rangaistuksesta tai muusta rikoksen seuraamuksesta, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi.

Myös henkilötunnuksen käsittely on tarkoin säänneltyä. HeTiL:n 3 luvun 13 §:ssä vakuutustoiminnasta on tästäkin asiasta erityismaininta, jonka perusteella vakuutuslaitoksella on oikeus käsitellä henkilötunnusta. Rekisterinpitäjän on kuitenkin huolehdittava siitä, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

2.4 Rekisteröidyn oikeus tietää häntä koskevista merkinnöistä

Henkilötietolain 6 luvun 26 §:n mukaan jokaisella on salassapitosäännösten estämättä oikeus tiedon etsimiseksi tarpeelliset seikat ilmoitettuaan saada tietää, mitä häntä kos-

kevia tietoja henkilörekisteriin on tallennettu tai, ettei rekisterissä ole häntä koskevia tietoja. Rekisteröidylle tulee samalla ilmoittaa rekisterin säännönmukaiset tietolähteet sekä, mihin rekisterin tietoja käytetään ja säännönmukaisesti luovutetaan. Tähänkin pykälään löytyy poikkeuksia HeTiL:n 6 luvun 27 §:stä, mutta ne eivät vaikuta vakuutusyhtiön toimintaan. Rekisteröidyllä on lisäksi oikeus vaatia virheellisen tiedon oikaisua.[7]

2.5 Tietosuojaviranomainen

Suomessa tietosuojaviranomaisen tehtäviä hoitaa kaksi eri viranomaista. Henkilötietojen suojaa koskevien asioiden käsittelyä on hoitanut vuodesta 1987 tietosuojalautakunta ja tietosuojavaltuutettu.

Tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain mukaan:

> *”Tietosuojavaltuutetun tehtävänä on käsitellä ja ratkaista henkilötietojen ja luottotietojen käsittelyä koskevat asiat siten kuin henkilötietolaissa ja luottotietolaissa säädetään sekä hoitaa muut mainituista laeista johtuvat tehtävät. Lisäksi sen tehtävänä on seurata näiden tietojen käsittelyn yleistä kehitystä ja tehdä tarpeelliseksi katsomiaan aloitteita ja huolehtia toimialaansa kuuluvasta tiedotustoiminnasta ja henkilötietojen käsittelyyn liittyvästä kansainvälisestä yhteistyöstä. Tietosuojavaltuutetulla on toimivalta antaa henkilötietojen käsittelyä koskevaa yleistä ohjausta ja neuvontaa sekä valvoa henkilötietojen käsittelyä henkilötietolain tavoitteiden toteuttamiseksi.”*

Tietosuojaviranomaiset toimivat yhteistyössä muiden EU:n jäsenvaltioiden tietosuojaviranomaisten kanssa.

Euroopan unionin lainvalvontayhteistyövirastosta annetun lain (214/2017) 5 §:n mukaan tietosuojavaltuutettu on kansallinen valvontaviranomainen. Kansallisen valvontaviranomaisen on valvottava, että jäsenvaltion suorittama henkilötietojen siirto, haku ja mikä tahansa toimittaminen on luvallinen, ja tutkia, loukkaako tällainen siirto, haku tai toimittaminen asianomaisten rekisteröityjen oikeuksia. Tietosuojavaltuutetun ohella toisena tietosuojaviranomaisena toimii tietosuojalautakunta.

[7] Tietosuojavaltuutetun toimisto 2017a, 7

2.6 Tietoturvallisuus

Henkilötietolain 7 luvun 32 §:n mukaan: ”rekisterinpitäjällä on velvollisuus toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.” Henkilötietolakia sovelletaan myös verkossa tapahtuvaan henkilötietojen käsittelyyn.[8]

HeTiL:n 7 luvun 33 §:n mukaan, jos henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessa on saanut tietää jotain toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei näitä tietoja saa ilmaista sivulliselle. Rekisterinpitäjän tulee vastata tietojen oikeellisuudesta ja ajantasaisuudesta. Hänellä on tietojen osalta vaitiolovelvollisuus ja velvollisuus suojata tiedot niin, ettei tiedot päädy asiattomille.[9] Lain 34 §:n mukaan rekisteri, joka ei ole enää tarpeellinen rekisterinpitäjän toiminnan kannalta, on hävitettävä.

[8] Tietosuojavaltuutetun toimisto 2017a, 5
[9] Pirinen ja Honkanen 2015, 55

3 TIETOSUOJAN SÄÄNTELYYN TULEVAT MUUTOKSET

3.1 Yleistä

Euroopan unionin yleinen tietosuoja-asetus tulee vahvistamaan säännöt luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä sekä säännöt, jotka koskevat henkilötietojen vapaata liikkuvuutta. Asetus suojelee luonnollisten henkilöiden perusoikeuksia ja –vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan. Henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.[10]

Tietosuoja-asetuksen lisäksi Euroopan parlamentti ja neuvosto ovat luoneet uuden direktiivin (EU) 2016/680. Kyseinen direktiivi on annettu luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.[11] Direktiivi koskee siis viranomaisten toimintaa, jonka vuoksi opinnäytetyössä ei perehdytä enempää kyseiseen direktiiviin.

EU:n tietosuojalainsäädännön uusiminen on lähtenyt liikkeelle jo vuonna 2012. Lainsäädäntö on jäänyt tältä osin jälkeen kehityksestä, eikä se enää vastaa globaalin tietoympäristön muuttuneita olosuhteita.[12] Monet asiat tulevat säilymään ennallaan, mutta tietosuoja-asetus tuo myös paljon uusia velvoitteita. Tämä vaatii rekisterinpitäjiltä ja henkilötietojen käsittelijöiltä valmistautumista. Mikäli asetusta rikkoo, siitä voi seurata erilaisia sanktioita.

Uuden lainsäädännön tavoitteena on parantaa henkilötietojen suojaa ja rekisteröidyn oikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin ja haasteisiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa sekä edistää digitaalisten sisämarkkinoiden kehittymistä.[13] Uudistuksen lähtökohtana on riskipohjainen lähestymistapa. Tarkoituksena on, että otetaan huomioon henkilötietojen käsittelyyn liittyvät riskit. Tällä halutaan taata henkilötietojen suojan korkea taso, varsinkin silloin, kun

[10] EUR-Lex 2016, 1 luku 1 artikla
[11] Euroopan parlamentin ja neuvoston direktiivi 2016
[12] Eduskunta 2017
[13] Tietosuojavaltuutetun toimisto 2017b

tietoja käsitellään korkean riskin toiminnassa, eli esimerkiksi henkilön terveystietojen käsittelyssä.[14] Oikeusministeriön asettama työryhmä ehdottaa, että Suomen lainsäädäntöön säädettäisiin uusi henkilötietojen suojaa koskeva yleislaki, jota kutsuttaisiin nimellä tietosuojalaki. Yleislaki on laki, jota sovelletaan, jollei muualla laissa toisin säädetä. Laki tulisi kumoamaan nykyisen henkilötietolain sekä lain tietosuojalautakunnasta ja tietosuojavaltuutetusta.[15]

Hallituksen esitys uudesta tietosuojalaista annettiin 1.3.2018. Esityksessä ehdotetaan, että Suomen lainsäädäntöön annetaan tietosuojalaki. Kyseinen laki täydentäisi ja täsmentäisi Euroopan unionin yleistä tietosuoja-asetusta. Esityksessä ehdotetaan, että samalla kumottaisiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Kyseessä olisi yleislaki, jota sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa. Lisäksi tulisi tehdä muutoksia rikoslakiin sekä sakon täytäntöönpanosta annettuun lakiin. Näiden lakien on tarkoitus tulla voimaan 25.5.2018, eli samana päivänä, jolloin Euroopan unionin yleistä tietosuoja-asetusta ryhdytään soveltamaan jäsenvaltioissa. Ehdotettu tietosuojalaki muodostuu erinäisistä yleistä tietosuoja-asetusta täydentävistä pykälistä ja sitä tulisi lukea rinnakkain yleisen tietosuoja-asetuksen kanssa.[16]

[14] Keskuskauppakamari 2016
[15] Oikeusministeriö 2017a
[16] HE 9/2018

Kuvio 1. Tietosuoja-asetuksen yleiset muutokset (Euroopan unionin neuvosto).

3.2 Tietosuoja-asetuksen soveltaminen

Yleistä tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä lisäksi sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.[17]

Kyseistä asetusta ei kuitenkaan sovelleta henkilötietojen käsittelyyn kaikissa tilanteissa. Esimerkiksi henkilötietojen käsittely, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu Euroopan unionin lainsäädännön soveltamisalaan tai käsittely, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa, ovat tilanteita, joissa tätä asetusta ei tulla soveltamaan.[18]

Riippumatta siitä, suoritetaanko henkilötietojen käsittely unionin alueella vai ei, sovelletaan tätä asetusta henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä. [19]

[17] EUR-Lex 2016, 1 luku 2 artikla
[18] EUR-Lex 2016, 1 luku 2 artikla
[19] EUR-Lex 2016, 1 luku 3 artikla

Tietosuoja-asetukseen valmistautuessa on omassa organisaatiossa hyvä käydä läpi ainakin seuraavat kohdat:

1. pitääkö organisaatioon nimittää tietosuojavastaava
2. miten organisaatiossa käsitellään henkilötietoja: henkilötietojen käsittelyn vaiheet keräämisestä hävittämiseen tulee dokumentoida
3. millä perusteella organisaatio ylipäätään käsittelee henkilötietoja
4. minkälaisia riskejä henkilötietojen käsittelyyn liittyy organisaatiossa: mitä riskejä voitaisiin minimoida
5. miten organisaatio noudattaa tietosuoja-asetuksessa määriteltyjä rekisteröityjen oikeuksia
6. tietoturvasta huolehtiminen: henkilötietojen tietoturvaloukkauksista täytyy jatkossa aina ilmoittaa
7. toimeksiantosopimusten tulee vastata asetuksessa säädettyjä ehtoja, mikäli organisaatio on ulkoistanut henkilötietojen käsittelyyn liittyviä tehtäviä
8. jos organisaatio toimii usean EU:n jäsenmaan alueella, tulee sille määritellä johtava valvontaviranomainen
9. lasten erityisaseman huomiointi organisaatiossa: jatkossa lapsi tarvitsee huoltajan tai muun vanhempainvastuunkantajan suostumuksen tai valtuutuksen tietoyhteiskunnan palveluiden käyttöön.[20]

Yleisen tietosuoja-asetuksen tietoyhteiskunnan palveluihin liittyvää lapsen suostumusta koskevassa 8 artiklan 1 kohdan mukaan ”henkilötietojen käsittelyn perustuessa suostumukseen ja kun kyseessä on tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle, lapsen henkilötietojen käsittely on lainmukaista, jos lapsi on vähintään 16-vuotias.” Mikäli lapsi on alle 16 vuotias, tällainen käsittely on lainmukaista vain, jos lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen tai valtuutuksen. Jäsenvaltiot voivat säätää tätä tarkoitusta koskevasta alemmasta iästä, mutta ikäraja saa kuitenkin alimmillaan olla 13 vuotta.

Suomessa tarkka ikäraja ei ole tässä vaiheessa vielä selvillä, mutta se tulee kuitenkin olemaan 13 ja 16 ikävuoden välissä. Ehdotusta hallituksen esitykseksi valmistelleen työryhmän järjestämässä kuulemistilaisuudessa esitetyissä puheenvuoroissa sekä saaduissa lausunnoissa korostettiin internetin merkitystä nuorille ja katsottiin, että se tarjoaa nuorille ympäristön itseilmaisun sekä ihmissuhdetaitojen kehittämiseen. Muiden

[20] Tietosuojavaltuutetun toimisto 2017b

pohjoismaiden ratkaisut asiassa huomioon ottaen ja lausuntokierrokselta saadun palautteen perusteella hallituksen esityksessä ikärajaksi ehdotetaan 13 vuotta.[21]

3.3 Tietosuojavastaava

Jotta tietää, tuleeko omassa organisaatiossa nimittää tietosuojavastaava, on seuraavassa listassa mainittu tilanteet, joissa organisaatiolla on velvollisuus nimittää tietosuojavastaava:

- kun kyse on julkisen sektorin toimijasta, joka ei ole tuomioistuin
- kun organisaation ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- kun organisaation ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.[22]

Tietosuojavastaavalla tulee olla riippumaton asema siinä organisaatiossa, jossa hän toimii tietosuojavastaavana. Kyseessä voi olla rekisterinpitäjän tai –käsittelijän palkkalistoilla oleva tai ulkoistettu henkilö. Jotta voidaan nimittää tietosuojavastaavaksi, tulee henkilöllä olla tietosuojalainsäädäntötuntemus, lain vaatimusten soveltamisosaaminen ja alan käytäntöjen tuntemus.[23]

Hänen tulee raportoida suoraan rekisterinpitäjän tai –käsittelijän ylimmälle johdolle. Tietosuojavastaava tulee ottaa asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin. Tähän tehtävään valitulle täytyy taata tarvittavat resurssit sekä asianmukainen pääsy henkilötietoihin ja niiden käsittelytoimiin. Tietosuojavastaava tekee yhteistyötä useiden organisaation yksiköiden kanssa ja hänellä tulee olla julkinen yhteyspiste valvontaviranomaisen ja rekisteröityjen suuntaan. Tehtävissä tulee noudattaa salassapitovelvollisuutta. Tietosuojavastaavaa ei saa erottaa tai rangaista tietosuojavastaavan tehtävien hoitamisen vuoksi. Näiden tehtävien lisäksi hän voi suorittaa muitakin tehtäviä mutta kuitenkin niin, ettei niistä aiheudu eturistiriitoja.[24]

[21] HE 9/2018
[22] Oikeusministeriö 2017b, 34
[23] Valtiovarainministeriö 2016, 19
[24] Valtiovarainministeriö 2016, 19

Tietosuojavaltuutetun tehtäviin kuuluu:

- asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa
- organisaation neuvonta ja ohjaus tietosuojaan liittyvissä kysymyksissä
- dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta
- ilmoitusvelvollisuuden toteutumisen seuranta
- vaikutustenarviointien tekemisen tukeminen ja valvonta
- yhteistyö valvontaviranomaisen kanssa
- tietosuojan tietoisuusohjelman rakentaminen ja sen kouluttaminen henkilöstölle
- rekisteröityjen oikeuksien toteuttamisen tukeminen
- käsittelytoimiin liittyvän riskin asianmukainen huomiointi tehtävien suorittamisessa.[25]

Tietosuojavaltuutetun toimistossa toimisi valtuutettujen lisäksi asiantuntijalautakunta. Tietosuojavaltuutetun toimisto olisi edelleen nykytilaa vastaavasti eduskunnan oikeusasiamiehen ja valtioneuvoston oikeuskanslerin ylimmän laillisuusvalvonnan sekä valtiontalouden tarkastusviraston valvonnan piirissä. Tietosuojavaltuutetun päätökseen saisi jatkossakin hakea muutosta valittamalla hallinto-oikeuteen siten kuin hallintolainkäyttölaissa säädetään. Vastaavasti hallinto-oikeuden päätökseen saisi säännösehdotuksen mukaan jatkossakin hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää asialle valitusluvan.[26]

3.4 Henkilötietojen käsittelyn periaatteet

Henkilötietojen suhteen tulee noudattaa seuraavia vaatimuksia:

1. henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi;
2. tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla;
3. käsittely on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään;

[25] Valtiovarainministeriö 2016, 19
[26] HE 9/2018

4. henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; tätä varten rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä;
5. tiedot on säilytettävä sellaisessa muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten;
6. tietoja 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.[27]

Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä näitä tietoja saa käsitellä myöhemmin näiden käyttötarkoitusten kanssa yhteensopimattomalla tavalla. Henkilötietojen tulee olla asianmukaisia, olennaisia ja tarpeellisia niiden käsittelytarkoituksen kannalta. Henkilötietoja ei siten voi kerätä esimerkiksi siltä varalta, että niiden käyttö voisi myöhemmin olla hyödyllistä.[28]

3.5 Henkilötietojen käsittelyn lainmukaisuus

Henkilötietojen käsittely on lainmukaista vain, kun vähintään yksi seuraavista edellytyksistä täyttyy:

1. rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn;
2. käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
3. käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamista varten;
4. käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
5. käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;

[27] EUR-Lex 2016, 2 luku 5 artikla
[28] HE 9/2018

6. käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi silloin kun henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja –vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi. Tätä kohtaa ei kuitenkaan sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtävänsä yhteydessä.[29]

Kuten nyt Suomessa voimassa olevassa henkilötietolain kolmannessa luvussa on säädetty arkaluontoisten tietojen käsittelystä, myös EU:n yleisen tietosuoja-asetuksen mukaan erityisiä henkilötietoryhmiä koskevien tietojen käsittely on kiellettyä. Näitä tietoja ovat sellaiset henkilötiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.[30] Tähänkin asetuksen osaan tulee kuitenkin pysymään tietyt poikkeukset, joissa tätä kohtaa ei sovelleta.

3.6 Rekisteröidyn oikeudet

Rekisterinpitäjän tulee pystyä toimittamaan rekisteröidylle kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tiedot tulee toimittaa kirjallisesti tai muulla tavoin ja yleensä myös sähköisessä muodossa. Mikäli rekisteröity pyytää, tiedot voidaan antaa myös suullisesti. Tämä edellyttää kuitenkin sitä, että rekisteröidyn henkilöllisyys on todennettu muulla tavoin.[31]

Rekisterinpitäjän tulee toimittaa rekisteröidylle tiedot tehdyn pyynnön johdosta ilman aiheetonta viivytystä. Joka tapauksessa tiedot tulee toimittaa kuukauden kuluessa siitä, kun rekisterinpitäjä on vastaanottanut pyynnön. Mikäli rekisterinpitäjä ei toteuta toimenpiteitä rekisteröidyn pyynnön perusteella, tulee tästä ilmoittaa viipymättä ja taas viimeistään kuukauden kuluttua pyynnön vastaanottamisesta. Samalla tulee ilmoittaa syyt siihen ja kerrottava, että rekisteröidyllä on mahdollisuus tehdä valitus valvontaviranomaiselle.[32]

[29] EUR-Lex 2016, 2 luku 6 artikla
[30] EUR-Lex 2016, 2 luku 9 artikla
[31] EUR-Lex 2016, 3 luku 12 artikla
[32] EUR-Lex 2016, 3 luku 12 artikla

Tietojen saamisen ja tästä aiheutuneiden toimenpiteiden tulee olla maksuttomia. Mikäli pyyntö on kuitenkin ilmeisen perusteeton tai kohtuuton, ja erityisesti jos niitä esitetään toistuvasti, voi rekisterinpitäjä joko periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea. Tällöin rekisterinpitäjän on osoitettava pyynnön perusteettomuus tai kohtuuttomuus.[33]

Rekisterinpitäjän tulee pystyä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Rekisteröity voi peruuttaa suostumuksensa milloin tahansa. Peruuttamisen tulee olla yhtä helppoa kuin sen antaminen.[34]

3.6.1 Tietojen oikaisu ja poisto

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä. Rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä. Tämä voi tapahtua esimerkiksi niin, että rekisteröity toimittaa lisäselvityksen.[35]

Kuten oikaisun osalta, rekisteröidyllä on myös oikeus saada rekisterinpitäjä myös poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä. Rekisterinpitäjällä on velvollisuus poistaa nämä tiedot, edellyttäen, että jokin seuraavista perusteista täyttyy:

1. henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne on kerätty tai joita varten niitä muutoin on käsitelty;
2. rekisteröity peruuttaa suostumuksen, johon tietojen käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta;
3. rekisteröity vastustaa käsittelyä, eikä käsittelyyn ole olemassa perusteltua syytä;
4. henkilötietoja on käsitelty lainvastaisesti;
5. henkilötiedot on poistettava rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi;
6. henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.[36]

[33] EUR-Lex 2016, 3 luku 12 artikla
[34] EUR-Lex 2016, 2 luku 7 artikla
[35] EUR-Lex 2016, 3 luku 16 artikla
[36] EUR-Lex 2016, 3 luku 17 artikla

Tietojen poisto eli niin kutsuttu ”oikeus tulla unohdetuksi”, on sisältynyt myös henkilötietolakiin, vaikka sitä itsessään ei ole kirjattu lakiin nimenomaisesti.[37]

3.6.2 Tietojen käsittelyn rajoittaminen

Rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä, jos kyseessä on jokin seuraavista tilanteista:

1. rekisteröity kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan siksi ajaksi, jonka aikana rekisterinpitäjä voi varmistaa tietojen todellisuuden;
2. käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojensa poistamista ja vaatii niiden käytön rajoittamista;
3. rekisterinpitäjä ei enää tarvitse kyseisiä tietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi;
4. rekisteröity on vastustanut henkilötietojen käsittelyä odottaessa sen todentamista; syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.[38]

3.6.3 Tietojen siirto järjestelmästä toiseen

Euroopan unionin virallisessa lehdessä julkaistun Euroopan unionin yleisen tietosuoja-asetuksen 3 luvun 20 artiklan mukaan:

> *”Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu, jos käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti.”*

[37] Oikeusministeriö 2017b, 25
[38] EUR-Lex 2016, 3 luku 18 artikla

3.7 Rekisterinpitäjän vastuu ja velvollisuudet

Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joiden avulla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan uutta tietosuoja-asetusta. Kyseisiä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.[39]

Rekisterinpitäjän tulee ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkaus tarkoittaa loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.[40]

Rekisterinpitäjän velvollisuudet kasvavat sen mukaan, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy. Henkilötietoja käsiteltäessä on pystyttävä osoittamaan, että rekisterinpitäjä noudattaa tietosuoja-asetusta. Käsittely on suunniteltava ja dokumentoitava.[41] Osoitusvelvollisuus on suuri muutos vanhaan lainsäädäntöön, sillä ennen ei ole tarvinnut pystyä osoittamaan, että säännöksiä noudatetaan. Tämä tulee todella parantamaan rekisteröidyn oikeuksia entiseen verrattuna.

Rekisterinpitäjien kannattaakin nähdä muutokset kilpailuetuna ja käyttää tarpeeksi resursseja muutosten eteenpäin viemiseen, jotta ne voivat välttyä sanktioilta ja käyttää muutosta jopa hyödyksi kovassa kilpailutilanteessa. Yleinen tietosuoja-asetus auttaa luomaan liiketoimintamahdollisuuksia ja se edistää innovointia muun muassa seuraavin keinoin:

1. jatkossa on yhteiset EU:n laajuiset säännöt, jonka arvioidaan säästävän 2,3 miljardia euroa vuodessa
2. tietosuojavaltuutettu, joka vastaa viranomaisten ja laajamittaisesti tietoja käsittelevien yritysten tietosuojasta
3. yhteys vain yhteen tietosuojaviranomaiseen, jonka vuoksi asiointi helpottuu ja yksinkertaistuu

[39] EUR-Lex 2016, 4 luku 24 artikla
[40] Oikeusministeriö 2017b, 32
[41] Tietosuojavaltuutetun toimisto 2017b

4. säännöt, jotka koskevat myös sellaisia EU:n ulkopuolelle sijoittautuneita yrityksiä, jotka tarjoavat tavaroita tai palveluja tai seuraavat henkilöiden käyttäytymistä EU:ssa
5. suotuisat säännöt innovaatioille, sillä tietosuoja huomioidaan tuotteissa ja palveluissa jo suunnitteluvaiheessa
6. yksityisyydensuojaa parantavat tekniikat ja salaus, jolloin tunnistetietoja korvataan keinotekoisilla tunnisteilla ja tiedot salataan niin, että vain valtuutetut osapuolet voivat lukea niitä
7. ilmoitusten poistaminen, sillä uudessa tietosuojalainsäädännössä poistetaan suurin osa ilmoitusvelvollisuuksista ja niihin liittyvistä kuluista sekä poistetaan henkilötietojen vapaan liikkuvuuden esteitä EU:n sisällä
8. rekisterinpitäjien tulee tehdä vaikutustenarviointeja, mikäli tietojenkäsittely voi aiheuttaa rekisteröidyn oikeuksien ja vapauksien kannalta korkean riskin
9. tietojen kirjaaminen, mikäli tietojen käsittely voi aiheuttaa henkilön oikeuksien ja vapauksien kannalta korkean riskin.[42]

3.8 Seuraamukset asetuksen noudattamatta jättämisestä

Jos EU:n yleistä tietosuoja-asetusta rikkoo, seuraa rekisterinpitäjälle tai henkilötietojen käsittelijälle siitä sanktio. Sanktion tulee olla kussakin yksittäisessä tapauksessa tehokas, oikeasuhteinen ja varoittava. Mikäli kyseeseen tulee hallinnollinen sakko, määrätään se kunkin yksittäisen tapauksen olosuhteiden mukaisesti. Kun sakon määräämisestä ja määrästä päätetään, on jokaisessa tapauksessa otettava huomioon seuraavat seikat:

1. sääntelyn rikkomisen luonne, vakavuus ja kesto, kyseisen tietojenkäsittelyn luonne, laajuus tai tarkoitus huomioon ottaen, sekä niiden rekisteröityjen lukumäärä, joihin rikkominen vaikuttaa ja heille aiheutuneen vahingon suuruus;
2. rikkomisen tahallisuus tai tuottamuksellisuus;
3. rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat toimet rekisteröidylle aiheutuneen vahingon lieventämiseksi;
4. rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste;
5. rekisterinpitäjän tai henkilötietojen käsittelijän mahdolliset aiemmat vastaavat rikkomukset;

[42] Euroopan unionin julkaisutoimisto 2016

6. yhteistyön aste valvontaviranomaisen kanssa rikkomisen korjaamiseksi ja sen mahdollisten haittavaikutusten lieventämiseksi;
7. henkilötietoryhmät, joihin rikkominen vaikuttaa;
8. tapa, jolla rikkominen tuli valvontaviranomaisen tietoon (ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä rikkomisesta);
9. jos kyseiselle rekisterinpitäjälle tai henkilötietojen käsittelijälle on aiemmin määrätty samasta asiasta toimenpiteitä, näiden toimenpiteiden noudattaminen;
10. hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen; ja
11. mahdolliset muut tapaukseen sovellettavat raskauttavat tai lieventävät tekijät.

Hallinnollinen sakko on tilanteesta riippuen joko enintään 10 000 000 euroa, tai jos kyseessä on yritys, edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta kaksi prosenttia sen mukaan, kumpi näistä määristä on suurempi. On myös sellaisia säännöksiä, joita rikkomalla voidaan määrätä enintään 20 000 000 euron sakko, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä on suurempi. Määrättävien sakkojen on oltava tehokkaita, jotta asetuksen säädöksiä todella noudatettaisiin.[43]

Sakkojen lisäksi jäsenvaltioiden tulee määrätä valvontaviranomaisen määräämiä asianmukaisia toimenpiteitä. Jos taas kyseessä on vain vähäinen asetuksen rikkominen tai jos määrättävä sakko olisi kohtuuton luonnolliselle henkilölle, voidaan sakon sijasta päätyä antamaan huomautus. Tässä tulee ottaa toki huomioon rikkomisen luonne ja muut seikat, jotka vaikuttavat rikkeen vakavuuteen. [44]

Valvontaviranomaisilla tulee olla kaikissa jäsenvaltioissa vastaavanlaiset tehtävät ja valtuudet. Valtuuksiin tulisi kuulua myös valtuus asettaa väliaikainen tai pysyvä tietojenkäsittelyn rajoitus, kuten käsittelykielto.[45] Jos rekisterinpitäjältä tai henkilötietojen käsittelijältä evättäisiin henkilötietojen käsittely edes väliaikaisesti, olisi sanktio varmasti niin tuntuva, ettei vastaavanlaisia erehdyksiä enää kävisi.

[43] EUR-Lex 2016, 8 luku 83 artikla
[44] EUR-Lex 2016, 150. kohta
[45] EUR-Lex 2016, 129. kohta

4 MUUTOSTEN KESKEISET VAIKUTUKSET VAKUUTUSYHTIÖN KORVAUSORGANISAATIOON

4.1 Yleistä

Kun uutta tietosuoja-asetusta aletaan soveltaa jäsenvaltioissa 25.5.2018, täytyy henkilötietojen säilytyksen ja käsittelyn olla sääntelyn mukaista. Henkilötietojen käsittely on ollut jo nykylainsäädännön puitteissa vakuutusyhtiöissä tarkkaa ja erittäin säänneltyä. Uusi tietosuojalaki tulee osittain tiukentamaan vanhoja käytäntöjä ja tekemään siitä vielä entistäkin tarkempaa. Uusi lainsäädäntö tarkoittaakin lähinnä vakuutusyhtiöissä huolellisuuden lisäämistä entisestään. Jokaisen yksilön tulee sisäistää huolellisuus henkilötietojen käsittelyssä. Vakuutusyhtiössä käsitellään asiakkaiden tietoja suurissa määrin päivittäin. Koska määrät ovat niin suuria ja tiedot sisältävät myös arkaluontoisia henkilötietoja, on erityisen tärkeää, että niiden käsittelyssä ollaan tarkkoja ja noudatetaan siihen liittyvää sääntelyä. Opinnäytetyössä käsitellään lakimuutoksen vaikutusta vain vakuutusyhtiön korvausorganisaatiota koskien ja työn ulkopuolelle jää kaikki muu toiminta vakuutusyhtiössä.

Vakuutusyhtiöillä on asiakkaista monenlaista tietoa, joka sisältää myös arkaluontoista tietoa. Esimerkiksi henkilökorvausorganisaatiossa käsitellään paljon vakuutetun tai korvauksenhakijan terveydentilaa ja erilaisia sairauksia. Uusi tietosuoja-asetus on jättänyt jäsenmaiden päättäjille sovellettavaa muun muassa juuri vakuutusyhtiön toimintaan liittyen, sillä vakuutusyhtiöille on tarpeellista jatkossakin saada kyseisiä tietoja vahinkoasioihin liittyen. Hallituksen esityksessä (9/2018) onkin mainittu seuraavaa:

> *”Nykylainsäädännön pohjalta on ilmeinen tarve säätää vakuutusyhtiön oikeudesta käsitellä eräitä erityisiin henkilötietoryhmiin kuuluvien tietojen lisäksi rikostuomioihon ja rikkomuksiin liittyviä tietoja vakuutusyhtiön vastuun selvittämiseksi. Vastaavasta oikeudesta säädetään tällä hetkellä henkilötietolaissa. Koska yleisestä tietosuoja-asetuksesta ei seuraa vakuutusyhtiölle suoraan oikeutta käsitellä eräitä erityisiin henkilötietoryhmiin kuuluvia ja 10 artiklassa tarkoitettuja tietoja vastuunsa selvittämiseksi, olisi ehdotettuun lakiin otettava käsittelyn oikeusperuste kyseistä*

> *tarkoitusta varten. Henkilötietolain tapaan säädettäisiin käsittelyn oikeusperusteesta oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi."*

Hallituksen esityksessä uudesta tietosuojalaista 6 §:ssä onkin kerrottu erityisiä henkilötietoryhmiä koskevasta käsittelystä seuraavasti:

> *"Tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovelleta vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi."*

Myös henkilötunnuksen käsittelystä on erityismaininta esitetyssä tietosuojalaissa. Lain 29 §:n mukaan henkilötunnusta saa käsitellä vakuutustoiminnassa. Sen käsittely on välttämätöntä vakuutustoiminnassa jo rekisteröidyn oikeusturvankin vuoksi.

4.2 Tunnistaminen

Asiakas voi olla yhteydessä korvauspalveluun monin eri tavoin. Millä tavoin hän onkaan palveluun yhteydessä, on tärkeää tunnistaa asiakas, mikäli kyse on hänen vakuutuksistaan tai mahdollisesta korvaushakemuksesta. Ilman asiakkaan tunnistamista ei voida olla varmoja onko kyseessä sellainen henkilö, jolle korvauspalvelun työntekijä saa kertoa vakuutustietoja. Jos asiakas haluaa hakea korvausta vakuutuksestaan, on työntekijän varmistettava, että hän asioi vakuutuksenottajan, hänen kotitalouteensa kuuluvan henkilön tai vakuutuksenottajan valtuuttaman henkilön kanssa.

On yleisesti olemassa kaksi eri tapaa tunnistaa henkilö; vahva tunnistaminen sekä muu tunnistaminen. Vahva tunnistaminen tarkoittaa sitä, että henkilöllisyys varmistetaan luotettavasta ja itsenäisestä lähteestä.[46] Tällainen tunnistamistapa on esimerkiksi passi, sähköinen tunnistautuminen verkkopankkitunnuksilla tai mobiilivarmenteella. Muu tunnistaminen taas tapahtuu loogisella päättelyllä ja sitä käytetään silloin, kun asiakas tunnistetaan hänen itsensä kertomien tietojen perusteella. Tämä on yleistä, kun asiakkaan kanssa asioidaan puhelimitse. Jatkossa on välttämätöntä, että tunnistamisesta jää jälki järjestelmään. Siksi onkin tärkeää, että tunnistamisprosessi kirjataan ylös.

[46] Vakuutusyhtiön sisäinen viestintä

Asiakkaan tunnistamisen täytyy olla uudistuksen voimaantullessa vielä nykyistäkin tarkempaa ja sen tulee tapahtua jokaisessa yhteydenotossa, jota asiakkaan ja vakuutusyhtiön välillä tapahtuu. Kun yhteydenotto tapahtuu soittamalla, on tärkeää olla varma siitä, kenen kanssa puhelimessa asioi. Asiakasta on tärkeä kuunnella, sillä asiakas kertoo yleensä yllättävän paljon itsestään jo heti puhelun alussa. Asiakkaan tunnistamiseen tulee kuitenkin soveltaa useampaa tunnistetietoa, sillä esimerkiksi pelkkä nimi tai henkilötunnus eivät takaa sitä, että puhelimen toisessa päässä on juuri se henkilö, jonka tiedot asiakas antaa. Yleinen käytäntö on, että asiakas tulee tunnistaa vähintään kolmen eri tiedon avulla. On tärkeää, ettei asiakkaalta kysytä johdattelevia kysymyksiä, vaan kysymysten tulee nimenomaan olla avoimia. Esimerkkejä yleisimmistä tunnistustiedoista:

- asiakkaan koko nimi
- henkilötunnus
- osoite, postinumero ja postitoimipaikka.

Mikäli asiakas on niin sanottu ”turvakieltoasiakas”, tulee hänet tunnistaa eri tavalla. Keskustelussa ei saa käsitellä asiakkaan osoitetietoa tai kotipaikkaa. Turvakieltoasiakas on henkilö, jolle maistraatti voi henkilön omasta pyynnöstä määrätä, ettei hänen kotikunta- tai osoitetietojaan saa antaa väestötietojärjestelmästä muille kuin viranomaisille. Tällöin henkilöllä on jokin perusteltu syy epäillä oman tai perheensä turvallisuuden olevan uhan alla.[47] Turvakieltoasiakkaan tunnistamiseen varmin tapa on pyytää asiakasta tunnistautumaan vakuutusyhtiön verkkopalvelussa, jonne kirjaudutaan omilla verkkopankkitunnuksilla tai mobiilivarmenteella. Tällöin vakuutusyhtiön työntekijä näkee, kun asiakas on kirjautunut kyseiseen palveluun, jonka jälkeen he voivat jatkaa asiointia normaalisti. Turvakieltoasiakkaan tunnistamisen tulee siis aina olla vahvan tunnistamisen mukaista.

Turvakieltoasiakkaan lisäksi sellainen asiakas, jolle on aina suoritettava vahvan tunnistamisen mukaiset toimenpiteet, on sellainen henkilö, jolla on osoitteenluovutuskielto. Tällaisen asiakkaan kanssa keskustellessa ei saa käydä ilmi asiakkaan osoite tai asuinpaikka missään muodossa. Asiakas on siis tunnistettava esimerkiksi niin, että hän kirjautuu vakuutusyhtiön verkkopalveluun aivan kuten turvakieltoasiakas. Vain tällä tavalla työntekijä voi varmistua siitä, että on yhteydessä oikean henkilön kanssa.

[47] Maistraatti

Jos asiakkaan kanssa on oltu usein yhteydessä esimerkiksi vahinkoasiaan liittyen, jo pelkkä äänitunnistaminenkin voi riittää. Mikäli kyse on vahinkoasian hoidosta, voi asiakkaan tunnistamiseen käyttää myös vahinkoon liittyviä kysymyksiä, kuten esimerkiksi: ”Mikä on vahingoittuneen ajoneuvosi rekisterinumero?” tai jokin muu tilanteeseen sopiva kysymys. Jos kyseessä on asiakastapaaminen, voi tunnistautuminen tapahtua kuten edellä on mainittu tai pyytämällä virallista henkilöllisyystodistusta.

Jos vakuutusyhtiön työntekijä on edelleen epävarma asiakkaan henkilöllisyydestä, tulee asiakas ohjata kirjautumaan verkkopalveluun tai käyttää omaa harkintakykyä. Myös oman osaston muilta työntekijöiltä tai esimieheltä voi pyytää apua tilanteen selvittämiseen. Mikäli yhteisymmärrykseen ei päästä, voi asiakasta aina kuunnella ja auttaa parhaansa mukaan, mutta asiakkaan yksityiskohtaisia vakuutus- tai korvaustietoja ei voi antaa, ellei asiakasta ole varmuudella todennettu siksi, joka hän ilmoittaa olevansa.

Yhteydenotto voi tulla myös sähköpostitse. Tällöin kannattaa pitää mielessä, vastaako sähköposti kaikilta osin asiakkaamme tietoja. Jos tästä on epäilys, voi asiakasta taas ohjata verkkopalveluun, jossa hän pystyy tunnistautumaan omilla verkkopankkitunnuksillaan. Asiakkaalle voi myös soittaa ja tunnistaa hänet puhelimitse.

Yhteydenotto voi asiakkaan lisäksi tulla esimerkiksi viranomaiselta, toisesta vakuutusyhtiöstä tai yhteistyökumppanilta. Mikäli kyseessä on henkilö, jonka kanssa on usein tekemisissä, voi pelkkä äänitunnistaminen riittää. Aina kannattaa selvittää, mihin kyseinen tiedustelu perustuu. Yleensä puhelussa käy luontevasti ilmi tietoja, joiden perusteella voi varmistua henkilöstä. Myös puhelinnumero kertoo yhteydenottajasta. Korvauspalvelun työntekijä voi myös pyytää henkilöä lähettämään tyhjän sähköpostin organisaationsa sähköpostiosoitteesta, jonka avulla voi helposti ja nopeasti nähdä, keskusteleeko todella sellaisen henkilön kanssa, joka puhelimessa kertoo olevansa.

4.3 Henkilötietojen säilytys

Kaikki henkilökohtaiset tiedot, joita työntekijät saattavat säilyttää yrityksen tuotantojärjestelmien ulkopuolella, tulee poistaa. Henkilökohtaiset tiedot ovat tietoja, jotka voidaan suoraan tai epäsuoraan yhdistää johonkin henkilöön. Tällaisia tietoja ovat esimerkiksi nimi, osoite, henkilötunnus tai muut henkilöllisyyteen liittyvät seikat.

On tärkeää muistaa, että tämä koskee asiakastietojen lisäksi myös työntekijöitä koskevia tietoja. Tietoja on saatettu säilyttää esimerkiksi henkilökohtaisissa- sekä ryhmäsähköpostilaatikoissa, jaetuissa tietokoneen kansioissa, oman työkoneen työpöydällä, Dropbox-sovelluksessa, yrityksen sisäisissä Yammer-ryhmissä, henkilökohtaisessa arkistossa, Skype-keskustelujen tallennuksissa, tekstiviesteissä tai USB-muistikortilla.

Tallennuspaikkoja on useita ja nyt ennen uuden lainsäädännön voimaantuloa onkin erittäin tärkeää, että jokainen korvausorganisaation työntekijä käy tarkkaan läpi kaikki nämä mahdolliset paikat ja poistaa kaikki nämä tiedot, jotka voidaan jotenkin yhdistää johonkin henkilöön. Esimerkiksi sähköpostiviestit asiakkaiden kanssa, korvauspäätökset sekä asiakastyytyväisyyskyselyt sisältävät näitä henkilökohtaisia tietoja, joita ei saa jatkossa säilyttää. Mikäli jotkut näistä dokumenteista ovat sellaisia, että ne täytyy säilyttää, tulee ne siirtää tuotantojärjestelmiin. Sovelluksen, johon tietoja tallennetaan, tulee olla sellainen, jossa on tietojen poisto- tai anonymisointiominaisuus. [48]

Vakuutusyhtiöt tai muutkaan rekisterinpitäjät eivät saa säilyttää henkilötietoja pidempään kuin se on tarpeen kyseisten tietojen alkuperäisen käyttötarkoituksen kannalta. Tämän vuoksi yritykset ovat määritelleet yleisesti noudatettavat säilytysajat, jotka on viety kyseisiin järjestelmiin, joissa henkilötietoja säilytetään. Vain sellaisia henkilötietoja saa tallentaa, jotka ovat asian käsittelyn kannalta välttämättömiä. Se, että tiedot saattavat mahdollisesti tulla tarpeellisiksi jossain vaiheessa, ei ole riittävä syy kyseisten tietojen tallentamiselle.[49]

4.4 Tietosuoja

Tietosuojaan liittyy suurelta osin sähköpostin turvallinen käyttö. Ensisijaisesti kommunikoinnin asiakkaan kanssa olisi hyvä tapahtua suljettujen palveluiden kautta, kuten yrityksen verkkopalvelun kautta, johon kirjaudutaan vahvan tunnistautumisen tavoin. Mikäli tämä ei ole mahdollista tai asiakas haluaa kommunikoida välttämättä sähköpostin kautta, on tärkeää, että sähköpostitse asioitaessa noudatetaan erityistä varovaisuutta.

Kun sähköpostia lähetetään ulkopuolisille ja jos sähköposti sisältää arkaluontoisia henkilötietoja, tulee varmistaa, että sähköposti on suojattu. Helpoin tapa suojata sähköpostiviestit, on käyttää suojattua sähköpostijärjestelmää. Yrityksillä on käytössään erilaisia

[48] Vakuutusyhtiö X:n sisäinen viestintä
[49] Vakuutusyhtiö X:n sisäinen viestintä

tapoja suojata sähköpostinsa. Yleensä, jos lähettää viestin yrityksen sisällä, ovat viestit suojattuja automaattisesti. Tällöin erillisiä suojaustoimia ei vaadita.

Uusi Euroopan unionin yleinen tietosuoja-asetus vaatii, että vain sellaiset työntekijät, joille on annettu valtuudet, saavat nähdä tarkempia henkilötietoja. Tämän vuoksi työntekijöiden valtuuksia tulee päivittää ennen muutosta. Lähtökohtaisesti valtuudet jaetaan vain niihin järjestelmiin ja tiedostoihin, joihin juuri kyseisen henkilön on päästävä toimenkuvansa vuoksi.

Jatkossa on myös pystyttävä osoittamaan, että vakuutusyhtiössä noudatetaan tietosuoja-asetusta. Tämän vuoksi on tärkeää, että henkilötietojen käsittely ja tallettaminen on suunniteltua. Toiminta on dokumentoitava niin, että valvontaviranomaisen on helppo selvittää, onko toiminta asetuksessa olevan sääntelyn mukaista.

5 LOPUKSI

Tämän opinnäytetyön aiheena oli pääasiassa uusi Euroopan unionin yleinen tietosuoja-asetus 2016/679 (EU). Työn tavoitteena oli verrata nykyisen henkilötietolainsäädännön ja uuden lainsäädännön eroja. Tarkoituksena oli lisäksi selvittää, miten nämä muutokset vaikuttavat vakuutusyhtiön korvausorganisaatioon ja sen käytäntöihin henkilötietojen suojaan liittyen.

Esitin työn alussa kysymyksen liittyen siihen, miten henkilötietoja tulee jatkossa käsitellä ja mitä velvollisuuksia rekisterinpitäjälle tämän muutoksen myötä muodostuu. Tavoitteenani oli, että tämän opinnäytetyön lukemisen jälkeen tulisi ymmärtää, miten henkilötietoja täytyy jatkossa käsitellä, sekä lisäksi mitä oikeuksia rekisteröidyllä on. Varsinkin rekisteröidyn oikeudet olivat ennen tämän työn tekoa itselleni täysin tuntematon asia.

Opinnäytetyössä voidaan huomata, että lainsäädännön uusiminen henkilötietojen ja tietosuojan osalta on välttämätöntä. Nopeasti muuttuva maailma on vaatinut lainsäädännön päivittämistä ajan tasalle näinkin arkaluontoisen asian suhteen kuin henkilötiedot ovat. Digitalisaatio ja globalisaatio ovat toki enimmäkseen hyvä asia, mutta ne luovat tietosuojaan myös suuria riskejä. Siksi onkin hyvä, että lainsäädäntöä on yhtenäistetty EU:n sisällä sekä myös kansallisessa lainsäädännössä.

Itselleni tuli opinnäytetyötä tehdessä yllätyksenä, että vaikka uutta asetusta aletaan soveltaa jäsenvaltioissa jo 25.5.2018, on kansallinen lainsäädäntö vielä kesken. Hallituksen esityksen julkaisu näin vähän aikaa aiemmin kuin lain pitäisi tulla voimaan, oli minulle yllätys. Toki kyseessä on EU:n yleistä tietosuoja-asetusta täydentävä yleislaki, jota tulkitaan rinnakkain Euroopan unionin asetuksen kanssa, joten on toisaalta ymmärrettävää, että hallituksen esitys ei tullut aiemmin julkiseksi. Mielestäni rekisterinpitäjille, jotka joutuvat ottamaan huomioon kyseisen muutoksen, olisi voinut olla hyödyllistä, mikäli hallituksen esitys olisi tullut hieman aiemmin julkiseksi.

Tein opinnäytetyöni teoreettisena tutkielmana, sillä mielestäni tästä aiheesta kirjoitettaessa se oli järkevin vaihtoehto. Pyrin pitämään tekstin mahdollisimman selkolukuisena ja sellaisena, että tekstin avulla on hyvä käydä aluksi nykylainsäädäntöä pääpiirteittäin läpi, jonka jälkeen voi siirtyä hieman tarkemmin analysoituun uuteen lainsäädäntöön. Lopuksi pohdin, miten muutos vaikuttaa vakuutusyhtiön korvausorganisaation toimintaan, sillä se on itselleni suuri mielenkiinnon aihe työni vuoksi. Sain itse opinnäytetyötä

tehdessäni paljon tietoa aiheesta ja koen, että minun on helpompi hahmottaa henkilötietojen lainsäätelyä jatkossa niin yleisellä tasolla kuin myös työssäni.

Jatkoa ajatellen olisi mielenkiintoista nähdä, miten muut EU:n jäsenvaltiot ovat kansallisella lainsäädäntötasolla ratkaisseet ne asetuksen kohdat, joiden sääntelyyn jätettiin kansallista liikkumavaraa. Uutena tutkimusaiheena voisi olla esimerkiksi se, miten Euroopan unionin yleisen tietosuoja-asetuksen sääntelyyn jätettyä jäsenvaltiokohtaista liikkumavaraa on lähdetty soveltamaan jäsenvaltioissa.

LÄHTEET

Asetus (EU) 2016/679: Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). EUR-Lex. Euroopan unionin virallinen lehti. Annettu 4.5.2016. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32016R0679.

Direktiivi (EU) 2016/680: Euroopan parlamentin ja neuvoston direktiivi luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. Euroopan unionin virallinen lehti. Annettu 4.5.2016. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32016L0680.

Eduskunta 2017: EU:n tietosuojauudistuksen kansallinen täytäntöönpano. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx. Viitattu 23.2.2018.

Euroopan unionin julkaisutoimisto 2016: Henkilötietojen suojaaminen (vuodesta 2018). Tiivistelmä. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=LEGISSUM:310401_2. Viitattu 24.3.2018.

Euroopan unionin neuvosto 2015: Infografiikka – Tietosuoja-asetus. http://www.consilium.europa.eu/fi/infographics/data-protection-regulation-infographics/. Viitattu 26.3.2018.

HE 9/2018: Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Annettu Helsingissä 1.3.2018. Saatavilla sähköisesti osoitteesta https://www.finlex.fi/fi/esitykset/he/2018/20180009#idp453416480.

Henkilötietolaki 523/1999. Annettu 22.4.1999. Saatavilla sähköisesti osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990523.

Keskuskauppakamari 2016: EU:n tietosuoja-asetus tulee – valmistaudu ajoissa. https://kauppakamari.fi/2016/03/31/eun-tietosuoja-asetus-tulee-valmistaudu-ajoissa/. Viitattu 1.3.2018.

Maistraatti: Turvakielto. https://www.maistraatti.fi/fi/Palvelut/kotikunta_ja_vaestotiedot/Turvakielto/. Viitattu 29.3.2018.

Oikeusministeriö 2017a: Työryhmä ehdottaa uutta tietosuojalakia. http://oikeusministerio.fi/artikkeli/-/asset_publisher/tyoryhma-ehdottaa-uutta-tietosuojalakia. Viitattu 23.2.2018.

Oikeusministeriö 2017b: Miten valmistautua EU:n tietosuoja-asetukseen? http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Viitattu 1.3.2018.

Pirinen, J. & Honkanen, J. 2015. Jokaisen oikeustieto. Helsinki: Sanoma Pro Oy.

Suomen perustuslaki 731/1999. Annettu 11.6.1999. Saatavilla sähköisesti osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10.

Tietosuojavaltuutetun toimisto 2017a: Ota oppaaksi henkilötietolaki! http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf. Viitattu 27.1.2018.

Tietosuojavaltuutetun toimisto 2017b: EU:n tietosuojauudistus. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#mitenvalmistautuatietosuoja-asetukseen. Viitattu 10.2.2018 ja 23.2.2018.

Valtioneuvosto 2017: EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf?sequence=1&isAllowed=y. Viitattu 26.1.2018

Valtiovarainministeriö 2016: EU-tietosuojan kokonaisuudistus. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128. Viitattu 24.3.2018.