Opinnäytetyö (AMK)

Liiketalous

2018

Sami Mannermaa

EU:N TIETOSUOJA-ASETUKSEN MUKANAAN TUOMAT VELVOLLISUUDET

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous

2018 | 30 sivua

Sami Mannermaa

EU:N TIETOSUOJA-ASETUKSEN MUKANAAN TUOMAT VELVOLLISUUDET

Tässä opinnäytetyössä tutkitaan EU:n tietosuoja-asetusta henkilötietoja päivittäin käsittelevän yrityksen näkökulmasta. Tietosuoja-asetus on hyvin laaja ja se sisältää paljon esimerkiksi vain julkishallintoa tai viranomaisia koskevaa sääntelyä. Tämän työn tavoitteena on selventää tietosuoja-asetusta sekä pyrkiä poimimaan siitä tärkeimmät huomionarvoiset seikat, joita yritys joutuu ottamaan liiketoiminnassa huomioon käsitellessään henkilötietoja.

Työn tärkeimpänä lähteenä toimii itse tietosuoja-asetus. Muita käytettyjä lähteitä ovat erilaiset henkilötietojen suojaa ja tietosuoja-asetusta koskevat verkkosivut, artikkelit, uutiset sekä kirjat.

Käsiteltäviin aiheisiin lukeutuvat rekisterinpitäjän velvollisuudet, tietojen käsittelyn lainmukaisuus, rekisteröidyn oikeudet, tietosuojavastaava, seloste käsittelytoimista sekä tietosuoja-asetuksen rikkomisesta määrättävät hallinnolliset sakot.

Opinnäytetyössä tullaan siihen johtopäätökseen, että koska tietosuoja-asetus on kaikessa laajudessaan hyvin vaikealukuinen, yrityksen liiketoiminnan sopeuttaminen siihen vaatii paljon aikaa sekä harkittuja toimenpiteitä. Tästä syystä yrityksen johdon tulisi varmistua siitä, että organisaation tietosuojavastaava on pätevä sekä tietoinen myös muusta asiaa koskettavasta lainsäädännöstä sekä sääntelystä. Ne säädökset, jotka yrityksen kannattaa ottaa erityisen tarkasti huomioon, koskevat yrityksen tiedonantovelvollisuuden täyttymistä, rekisteröidyn oikeuksien huomioon ottamista sekä henkilötietojen säilytystä ja käyttötarkoitusta.

ASIASANAT:

tietosuoja, tietosuojavastaava, henkilötieto, henkilörekisteri, rekisterinpitäjä, rekisteröity

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business

2018 | 30 pages

Sami Mannermaa

THE OBLIGATIONS SET BY THE GENERAL DATA PROTECTION REGULATION

In this thesis, we study the General Data Protection Regulation from the standpoint of an enterprise that processes personal data in its daily operation. Due to the extent of the Regulation it might be hard to interpret or find the essential information suited for one's needs. The goal of this thesis is to provide information about the Regulation in a concise and distinct way, so that enterprises will be able to easily gather the most relevant information to apply in their business activities and especially while processing any personal data.

The main information source used is the General Data Protection Regulation itself. Other sources include various books, websites, articles and news that cover the Regulation or protection of personal data in general.

Topics addressed in the thesis include the responsibilities of a controller, lawfulness of the data processing, rights of the data subject, data protection officer, records of processing activities and the administrative fines imposed for the infringement of the Regulation.

In conclusion, due to the complexity of the Regulation many enterprises will find it challenging to adapt to the legislation. It will take time and carefully planned steps to make sure every important aspect is considered. For this reason, the management should make sure that the chosen data protection officer is qualified for the task. Knowledge of other data protection related legislation is also recommended. Overall, the most important thing to consider when reviewing the processes within the enterprise, is making sure that the data subject knows what personal data is being used and for what purpose, while taking data subjects rights into account.

KEYWORDS:

data protection, data protection officer, personal data, personal data register, controller, data subject

SISÄLTÖ

1 JOHDANTO

Euroopan parlamentin ja neuvoston asetuksen yksilöiden suojelusta henkilötietojen käsittelyssä (jäljempänä tietosuoja-asetus tai asetus) keskeisenä tavoitteena on yhdenmukaistaa jäsenvaltioiden tietosuojalait sekä muu siihen liittyvä sääntely ja samalla helpottaa sähköisten palveluiden tarjoamista yli jäsenvaltioiden rajojen. Tarkoitus on samalla tehostaa henkilötietoja käsittelevien organisaatioiden tehokkuutta ja tuottavuutta – saaden aikaan kustannussäästöjä.[1] Asetus on tullut koko EU:n alueelle automaattisesti suoraan sovellettavaksi. Asetuksesta yleisesti käytetty lyhenne GDPR tulee englanninkielisistä sanoista General Data Protection Regulation. Henkilötietoja käsittelevien organisaatioiden on tullut niiden koosta riippumatta varautua uuden tietosuoja-asetuksen sääntelyyn annetun siirtymäajan puitteissa. Siirtymäaika on alkanut kun tietosuoja-asetus on lopullisesti hyväksytty Euroopan parlamentissa ja yrityksillä on ollut aikaa tehdä tarvittavat toimenpiteet ennen siirtymäajan päättymistä 25.05.2018. Asetuksen vastaisesta henkilötietojen käsittelystä voidaan määrätä yrityksen liikevaihdon perusteella määräytyviä, hyvin ankaria sanktioita. Nykyinen henkilötietolaki tullaan uudistamaan tietosuoja-asetusta täydentävällä uudella tietosuojalailla.[2]

Tietosuoja-asetuksen siirtymäajan puitteissa on julkaistu useita tutkimuksia, joissa on selvitetty tietosuoja-asetukseen valmistautumista suomalaisissa yrityksissä. Muun muassa Valtioneuvoston selvitys- ja tutkimustoiminnan artikkelisarjan osana julkaistussa kyselyssä kävi ilmi, että asetuksen laajuus sekä siirtymään annettu aikataulu on koettu etenkin pk-yrityksissä haastavaksi.[3] Tietosuoja-asetuksen haastavuudesta kertoo myös se, että vuonna 2016 Elisan ja Suomen yrittäjien teettämän tutkimuksen mukaan vain noin kolmannes mikro- ja pienyrityksistä tiesi tietosuoja-asetuksesta jonkin verran tai tunsi sen hyvin.[4]

Etenkin digitaalisia palveluta tarjoavien yritysten tietoturva on tänä päivänä paljon esillä julkisuudessa. Useissa medioissa on uutisoitu eri kokoisten yritysten joutuneen tietovuodon kohteeksi, jonka seurauksena henkilötietoja on vuotanut ulkopuolisten henkilöiden nähtäville. Muun muassa matkailualan yritys Orbitz on ilmoittanut joutuneensa tietomurron kohteeksi, jonka johdosta ulkopuolinen taho on saattanut päästä käsiksi palvelun

[1] Andreasson ym. 2017, 28
[2] Hanninen ym. 2017, 13-15
[3] Enroth, T. & Neuvonen R. 2017
[4] Elisan ja Suomen yrittäjien tutkimus suomalaisten pk-yritysten digitalisaation asteesta. 2016

käyttäjien henkilö- ja maksukorttitietoihin.[5] Suurista, tunnetuista yrityksistä Facebook on ollut paljon otsikoissa käytyä ilmi, että analytiikkayhtiö Cambridge Analytica on saattanut päästä käsiksi jopa 87 miljoonan Facebook-käyttäjän henkilötietoihin. Näiden tietojen käyttö ja myynti on yhdistetty muun muassa Yhdysvaltain presidentinvaalien tulosten manipulointiskandaaliin.[6] Suomessa tapahtuneista suurista tietovuodoista eniten otsikoissa ovat olleet Itä-Suomen yliopistoon sekä Työtehoseuran tietokentoihin tehdyt tietomurrot vuonna 2011. Noin 16 000 ihmisen henkilötiedot – jotka sisälsivät muun muassa osoitteita ja puhelinnumeroita – julkaistiin Internetissä kaiken kansan nähtäville ja niitä on käytetty Helsingin poliisin mukaan useissa petoksissa, petosten yrityksissä ja identiteettivarkauksissa.[7]

On luonnollista, että edellä mainittujen tapausten kaltaisten tietovuotojen julkisuuteen tulo vaikuttaa negatiivisesti asiakkaan luottamukseen kyseistä yritystä kohtaan. Tietosuojasta onkin tämän takia tullut yhä selvemmin yrityksen strategisen toiminnan keskeinen osa-alue. Kun yrityksen henkilöstö on tietosuojaosaavaa ja tehokkaasti, mutta tietoturvallisesti toimivaa, hyötyvät tästä sekä asiakkaat että yritys ja sen henkilöstö itse. Yrityksen henkilötietojen käsittelyn suunnitteleminen ja toteuttaminen tietosuoja-asetuksen säädöksiä noudattaen mahdollistaa onnistumisen digitaalisilla markkinoilla. Tietosuojan voidaan siis sanoa olevan digitalisaation mahdollistaja ja yrityksen menestystekijä.[8]

Tässä opinnäytetyössä käsitellään tietosuoja-asetuksen tärkeimpiä säännöksiä, jotka henkilötietoja käsittelevän yrityksen tulee ottaa huomioon kaikessa suorittamassaan henkilötietojen käsittelyssä. Työn suurimpana tietolähteenä toimii tietosuoja-asetus ja esimerkiksi opinnäytetyön kirjoitushetkellä vielä voimassa olevaa henkilötietolakia on käsitelty tässä työssä hyvin pintapuolisesti. Henkilötietolaki on voimassa niin kauan, kunnes se kumotaan 13.11.2018 eduskunnan käsittelyssä hyväksytyllä uudella tietosuojalailla.[9]

[5] Tivi. 2018
[6] Yle. 2018
[7] Savon Sanomat. 2017
[8] Andreasson ym. 2017, 19-20
[9] Tietosuojavaltuutetun verkkosivut. 2018

2 REKISTERINPITÄJÄN VELVOLLISUUDET

2.1 Henkilötietojen käsittelyä koskevat periaatteet

Tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyn periaatteista, jotka ovat pääpiireittän nykyisen henkilötietolain periaatteiden mukaiset. Näiden periaatteiden sisältöä on kuitenkin tarkennettu ja muutamia periaatteita on lisätty. Rekisterinpitäjän tulee varmistaa, että tietosuojaperiaatteita noudatetaan koko organisaatiossa kaikessa henkilötietojen käsittelyssä. Henkilötietojen käsittelyä koskevat periaatteet ovat seuraavat:[10]

a) Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
b) Käyttötarkoitussidonnaisuus ja täsmällisyys
c) Säilytyksen rajoittaminen ja tietojen minimointi
d) Eheys ja luottamuksellisuus
e) Rekisterinpitäjän osoitusvelvollisuus

Käytännössä rekisterinpitäjän hallussa olevien henkilötietojen on oltava kerätty jotakin tiettyä ja laillista tarkoitusta varten, eikä niitä saa käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Tietoja on käsiteltävä asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Käsiteltävän henkilötiedon määrä tulee myös rajoittaa suhteessa siihen, mikä on tarpeellista niihin tarkoituksiin, joita varten kyseessä olevia henkilötietoja käsitellään. Sellaista ylimääräistä henkilötietoa, jolla ei ole mitään käyttötarkoitusta, ei saa säilyttää eikä sitä saa käsitellä.[11]

Käsiteltävien henkilötietojen on oltava täsmällisiä sekä ajantasaisia, joten rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimeenpiteet sen varmistamiseksi. Epätarkat tai virheelliset henkilötiedot on poistettava tai korjattava heti, kun tieto niiden virheellisyydestä on saatu. Kaikki tiedot on säilytettävä sellaisessa muodossa, joka mahdollistaa rekisteröidyn tunnistamisen vain niin kauan kuin on tarpeellista käsittelyn tarkoitusten toteuttamista varten. Henkilötietoja on käsiteltävä sellaisella tavalla, että voidaan varmistua niiden turvallisuudesta ja että ne on suojattu luvattomalta käsittelyltä sekä tietojen häviämiseltä tai tuhoutumiselta.[12]

[10] Autio ym. 2017, 12
[11] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 5. artikla
[12] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 5. artikla

2.2 Osoitusvelvollisuus

Yksi keskeisimmistä ja eniten toimenpiteitä vaativista säännöksistä on rekisterinpitäjän osoitusvelvollisuus. Rekisterinpitäjän tulee käytännössä pystyä osoittamaan edellä mainittujen periaatteiden toteutuminen ja niiden noudattaminen oman organisaation sisällä. Osoitusvelvollisuus täytetään dokumentoimalla kaikki henkilötietojen käsittelyyn liittyvä käytäntö sekä sen toteuttaminen. Henkilötietolaissa on ollut riittävää, että asetettuja säännöksiä noudatetaan, eli dokumentoitivelvoite tulee täysin uutena asiana. Dokumentaatio on kirjaamisen lisäksi pidettävä ajan tasalla, eli asiakirjat ja käytännöt on päivitettävä aina tarpeen tullen. Rekisterinpitäjän tulisi käytännössä dokumentoida vähintään seuraavat tiedot: [12]

a) Tietosuojaorganisaatio (mukaan lukien tietosuojavastaava)
b) Käsiteltävät tietoryhmät
c) Käsittelyn perusteet
d) Henkilötietojen käyttötarkoitus
e) Henkilötietojen käsittelytapa

Mikäli organisaatiossa on aikaisemmin jouduttu pohtimaan joidenkin tiettyjen henkilötietotyyppien käsittelyn tai käsittelyssä noudatettavien toimintapojen tarpeellisuutta tai lainmukaisuutta, olisi hyvä kirjata ylös myös perustelut siitä, miksi käsittelyn on katsottu olevan tarpeellista ja sallittua. Tämä on erityisen tärkeää, mikäli käsitellään arkaluontoisia henkilötietoja. Organisaation tulisi myös kirjata ylös henkilötietojen säilytysajat ja millä perusteella käytössä oleviin säilytysaikoihin on päädytty. Suositeltavaa on listata myös kaikki ne tahot, joilta organisaatio saa tai joille organisaatio luovuttaa henkilötietoja. Muita mahdollisesti tärkeänä pidettäviä tietoja ovat annetut ja peruutetut henkilötietojen käsittelyn suostumukset, tietojen ajantasaisuuden varmistaminen ja päivittäminen, henkilötietojen käsitelyn mahdollinen ulkoistaminen sekä henkilötietojen suojaamista koskeva kuvaus. Tämä kuvauksen olisi hyvä sisältää tiedot henkilötietojen teknisestä suojasta – kuten esimerkiksi tilojen lukituksista ja kulkuoikeuksista – mutta mahdollisesti myös salassapito- ja salasanapolitiikasta, lokitiedoista sekä henkilöstön koulutuksesta.[13]

[13] Hanninen ym. 2017, 51-53

2.3 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetun tietosuojan periaatteella tarkoitetaan tietosuojaperiaatteiden huomioon ottamista jo palveluiden ja tuotteiden suunnitteluvaiheessa. Mahdollisten riskien realisoitumista ei odoteta, vaan ne tulee kartoittaa ja huomioida jo ennen esimerkiksi henkilötietojen käsittelyssä käytettävän ohjelmiston tai sen toimittajan valitsemista. Mikäli henkilötietojen käsittelyyn liittyy tavallista korkeampi riski, kuten esimerkiksi arkaluontoisia henkilötietoja käsitellessä, on tietosuojan huomioiminen suunnitteluvaiheessa erityisen tärkeää. Oletusarvoisen tietosuojan periaatteen huomioon ottaminen vaatii rekisterinpitäjältä sitä, että oletusarvoisesti käsitellään vain kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Huomioon on otettava myös kerättyjen tietojen määrä, käsittelyn laajuus sekä tietojen säilytysaika. Edellä mainittujen periaatteiden huomioon ottaminen mahdollisimman varhaisessa vaiheessa on organisaatiolle taloudellisesti kannattavampaa, kuin jo käytössä olevissa järjestelmissä havaittujen virheiden korjaaminen. Koko henkilökunnan kouluttaminen tietosuoja-asetukseen liittyen edistää omalta osaltaan näiden tietosuojakysymysten huomioon ottamista mahdollisimman aikaisin tuote- tai palvelukehityksen aikana.[14]

Rekisterinpitäjä pystyy osoittamaan edellä mainittujen vaatimusten noudattamisen käyttämällä esimerkiksi tietosuoja-asetuksen 42 artiklan mukaista sertifiointimekanismia. Tietosuojaneuvosto ja -komissio kannustavat organisaatioita näiden sertifikaattien käyttöönottoon. Sertifikaattien tarkoituksena on osoittaa, että henkilötietojen käsittelytoimia suoritettaessa on noudatettu tietosuoja-asetusta. Sertifioinnin voivat myöntää tähän tarkoitukseen solveltuvat sertifiointielimet tai toimivaltainen valvontaviranomainen. Tämä on kuitenkin vapaaehtoista, eikä tietosuoja-asetus velvoita sertifikaattien käyttöönottoon.[15]

[14] Hanninen ym. 2017, 54-55
[15] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 25 ja 42 artikla

3 TIETOJEN KÄSITTELYN LAINMUKAISUUS

3.1 Lainmukaisuus yleisesti

Henkilötietojen käsittely on tietosuoja-asetuksen mukaan lainmukaista, kun vähintään yksi asetuksessa määritellyistä edellytyksistä täyttyy. Edellytyksiä voivat olla suostumus, sopimus, lakisääteisyys, oikeutettu etu, rekisteröidyn tai muun luonnollisen henkilön elinärkeiden etujen suojaaminen, yleinen etu tai julkisen vallan käyttö. Edellä mainituista kahden viimeisen kohdan täyttyminen on pk-yrityksen kohdalla hyvin harvinaista, eikä niitä sen takia käydä tarkemmin läpi tässä opinnäytetyössä. Useimmat edellä mainituista edellytyksistä voivat täyttyä tai soveltua samanaikaisesti henkilötietojen käsittelyyn.[16]

Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely on oletusarvoisesti kielletty. Näihin lasketaan sellaiset tiedot, jotka koskevat rekisteröidyn etnistä alkuperää, poliittisia mielipiteitä, uskonnollista vakaumusta, seksuaalista käyttäytymistä tai muita vastaavia tietoja. Niiden käsittely voi kuitenkin olla lainmukaista, mikäli rekisteröity on esimerkiksi antanut nimenomaisen suostumuksen kyseisen tiedon käyttöön, jos käsiteltävät tiedot on nimenomaisesti saatettu julkiseksi rekisteröidyn toimesta tai mikäli käsittely on tarpeen jonkin tuomioistuimen lainkäyttötehtävien suorittamista varten.[17]

3.2 Suostumus

Suostumuksella tarkoitetaan rekisteröidyn antamaa vapaaehtoista, yksilöityä, tietoista ja ykseiselitteistä tahdonilmaisua, joka on annettava kirjallisesti tai suullisesti selkeästi suostumusta ilmaisevalla toimella. Esimerkkinä tällaisestä sähköisestä toimesta voidaan pitää valintaruudun itse henkilökohtaisesti rastittamista Internetsivulla tai kirjallisen suostumuslomakkeen täyttämistä. Suostumusta ei voi antaa esimerkiksi vaikenemalla tai jättämällä jokin toimi tekemättä. Verkkosivuilla käytettävien rastitusruutujen automaatinen täyttö on tällä perusteella kiellettyä tai ainakin hyvin kyseenalaista. Jos tietojen käsittelyllä on useampia tarkoituksia, tulee suostumus antaa erikseen kaikkia näitä käsittelytarkoituksia varten. Rekisteröidyllä tulee myös olla oikeus peruuttaa suostumuksena milloin

[16] Hanninen ym. 2017, 29
[17] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 9 artikla

tahansa ja sen peruuttamisen on oltava yhtä helppoa kuin sen antaminen.[18] Hyvin yleinen ja helppo tapa suostumuksen peruuttamisen tarjoamiseen on esimerkiki listätä yrityksen lähettämän sähköpostin alkuun tai loppuun linkki, jota klikkaamalla rekisteröity voi kieltää suoramarkinnoinoinnin tai peruuttaa aikaisemmin tilaamaansa uutiskirjeen.

3.3 Sopimus

Henkilötietojen käsittely on lainmukaista, mikäli se on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai tämän sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.[19] Sopimuksen täytäntöön panemiseksi voidaan laskea esimerkiksi verkkokauppaan rekisteröidyn henkilön postiosoitteen tai puhelinnumeron käsittely, jonka perusteella ostettu tavara voidaan toimittaa tilauksen tekijälle. Sopimuksen tekemistä edeltävien toimenpiteiden osalta esimerkkinä voidaan pitää tilannetta, jossa henkilö pyytää yhtä tai useampaa yritystä lähettämään tarjouksen haluamastaan tuotteesta tai palvelusta.

3.4 Lakisääteisyys

Henkilötietojen käsittely on lainmukaista, kun se on tarpeen jonkin rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Tämän lakisääteisyysvelvoitteen tulee perustua johonkin Euroopan unionin oikeudessa tai rekisterinpitäjään sovellettavan jäsenvaltion kansallisessa lainsäädännössä säädettyyn velvoitteeseen. Edellä mainitulla lakisääteisyysvalvoitteella voidaan tarkoittaa esimerkiksi osakeyhtiölaissa säädettyä asunto-osakeyhtiön velvollisuutta pitää yllä osakasluetteloa tai yhdistyslaissa säädettyä yhdistyksen velvollisuutta pitää yllä luetteloa sen jäsenistä. Työnantajaa koskevista lakisääteisistä velvoitteista voidaan mainita esimerkiksi työntekijöiden palkkatietojen ilmoittaminen sosiaali- tai veroviranomaisille, jolloin lakisääteinen peruste tietojen käsittelyä ja jakamista varten täyttyy.[20]

[18] Hanninen ym. 2017, 35-37
[19] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, alkukappale, kohta (40)
[20] Hanninen ym. 2017, 31

3.5 Oikeutettu etu

Oikeutetun edun katsotaan olevan olemassa esimerkiksi silloin, kun rekisteröidyn ja reskisterinpitäjän välillä on asianmukainen ja merkityksellinen suhde, kuten esimerkiksi rekisteröidyn ollessa rekisterinpitäjän asiakas tai työsuhteessa rekisterinpitäjään nähden. Oletuksena on, että asiakkaan tietoja voidaan käsitellä esimerkiksi tuotteiden toimittamiseksi tai asiakasviestinnän lähettämiseksi. Mikäli henkilötietojen suojaa edellyttävät rekisteröidyn edut tai oikeudet kuitenkin syrjäyttävät oikeutetun edut, ei henkilötietojen käsittely ole sallittua. On rekisterinpitäjän vastuulla vertailla oikeutetun ja rekisteröidyn oikeuksia. Kun kyseessä on alaikäinen lapsi, rekisteröidyn edut ja oikeudet syrjäyttävät oikeutetun edut paljon helpommin, kuin täysi-ikäisen rekisteröidyn kohdalla. Oikeutetun etua ei tule myöskään pitää kaiken sellaisen tiedon käsittelyperusteena, jonka käsittelyyn ei voida soveltaa mitään muita tietosuoja-asetuksessa mainittuja perusteita.[21]

Tietosuoja-asetuksessa on erikseen säädetty rekisteröityjen henkilötietojen käsittelyn suoramarkkinointitarkoituksessa kuuluvan oikeutetun edun piiriin. Suoramarkkinointia voidaan tällä perusteella kohdentaa potentiaalisille asiakkaille, kunhan vastaanottajille tiedotetaan mahdollisuudesta kieltää markkinointi. Suoramarkkinoinnin kielto-oikeus on aina saatettava rekisteröidyn tietoon selkeästi ja erillään muusta tiedotuksesta. Sähköisen suoramarkkinoinnin sääntelyyn ei tule varsinaisia muutoksia tietosuoja-asetuksen myötä, joten esimerkiksi etukäteisen suoramarkkinointiin suostumisen edellytys sähköpostisuoramarkkinoinnin lähettämiseksi säilyy ennallaan.[22]

[21] Hanninen ym. 2017, 32-34
[22] Hanninen ym. 2017, 34-35

4 REKISTERÖIDYN OIKEUDET

4.1 Rekisteröidyn oikeuksista yleisesti

Rekisterinpitäjän velvollisuutena on ottaa rekisteröidyn oikeudet huomioon henkilötietojen käsittelyssä sekä siihen liittyvien prosessien ja käytäntöjen suunnittelussa. Tietosuoja-asetuksessa säädetyt rekisteröidyn oikeudet vastaavat hyvin pitkälti henkilötietolain mukaisia oikeuksia, mutta niihin liittyvä sääntely on huomattavasti yksityiskohtaisempaa. Henkilötietoja käsittelevän organisaation onkin varmistuttava siitä, että jo käytössä olevat, henkilötietolain mukaiset toimintatavat mahdollistavat näiden oikeuksien toteuttamisen. Tarvittaessa toimintatapoihin on tehtävä muutoksia. Asetuksessa on säädetty myös täysin uusista rekisteröityjen oikeuksista. Käsittelyn oikeusperusteet vaikuttavat omalta osaltaan rekisteröidyllä oleviin oikeuksiin kunkin yksittäisen käsittelytapahtuman kohdalla.[23]

Rekisteröidyn oikeudet tulee saattaa rekisteröidyn tietoon sellaisella tavalla, että rekisteröity voi käyttää oikeuksiaan helposti. Organisaation on kuitenkin varmistuttava siitä, että vain rekisteröity itse voi käyttää näitä oikeuksia. Tämä tapahtuu tunnistamalla oikeuksiaan käyttävä asiakas esimerkiksi kuvallisesta henkilökortista tai ohjaamalla asiakas kirjautumaan omilla henkilökohtaisilla tunnuksillaan yrityksen verkkopalveluun, mikäli nämä tunnistamistavat soveltuvat yrityksen liiketoimintaan. Yritys voi myös pyytää rekisteröityä toimittamaan allekirjoitetun pyynnön postitse tai sähköpostise. Edellä mainittuun poikkeuksena ovat alaikäiset rekisteröidyt, joita edustaa määrätty huoltaja. Mikäli rekisteröity ei toimita tarpeellisia tietoja, voi yritys kieltäytyä toimimasta rekisteröidyn pyynnön mukaisesti. Kun asianmukainen pyyntö on vastaanotettu, tulee yrityksen toimittaa rekisteröidylle kuukauden sisällä tiedot niistä toimenpiteistä, joihin se on ryhtynyt rekisteröidyn esittämän pyynnön perusteella. Nämä tiedot tuee pyrkiä toimittamaan sähköisessä muodossa, ellei rekisteröity ole pyytänyt niitä esimerkiksi paperilla. Mikäli esitetty pyyntö on erityisen monimutkainen tai niitä on määrällisesti useampia, voidaan pyynnön toteuttamisen määräaikaa jatkaa enintään kahdella kuukaudella. Viivästymisen syyt sekä uusi määräaika tulee kuitenkin ilmoittaa rekisteröidylle kuukauden kuluessa pyynnön vastaanottamisesta. Pyynnön toteuttamisen tulee olla rekisteröidylle maksutonta, elleivät rekisteröidyn esittämät pyynnöt ole poikkeuksellisen perusteettomia tai kohtuuttomia.

[23] Autio ym. 2017, 23

Edellä mainituissa tapauksissa yritys voi joko periä kohtuullisen maksun tai kieltäytyä kokonaan suorittamasta esitettyä pyyntöä.[24]

4.2 Oikeus saada läpinäkyvää informaatiota

Henkilötietojen käsittelyn avoimuus on yksi tietosuoja-asetuksen peruspilareista ja siinä säädetäänkin henkilötietolakia tarkemmin rekisterinpitäjän tiedonantovelvollisuudesta. Asetuksessa on säädetty erikseen rekisteröidyn informoinnin luonteesta ja sisällöstä riippuen siitä, onko henkilötiedot kerätty suoraan rekisteröidyltä vai jotakin muuta kanavaa käyttäen. Silloin kun henkilötietojen käsittelyä koskevat tiedot on hankittu jotakin muuta kautta, tulee rekisterinpitäjän toimittaa pyydetyt tiedot kohtuullisen ajan kuluessa, mutta viimeistään kuukauden sisällä tietojen saamisesta. Mikäli näitä hankittuja tietoja käytetään viestintään rekisteröidyn kanssa, tulee tiedot toimittaa rekisteröidylle silloin kun niitä käytetään ensimmäisen kerran. Rekisterinpitäjän tulee toimittaa kaikki rekisteröidyn pyytämät tiedot helposti ymmärrettävässä ja selkeässä muodossa.[25]

Henkilötietolain mukaan rekisteröidyllä on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteri sisältää tai mikäli rekisterissä ei ole häntä koskevia tietoja. Rekisterinpitäjän on tällöin ilmoitettava myös rekisterin tietojen käyttötarkoitus sekä mihin kaikkialle näitä tietoja luovututetaan ja mistä niitä hankitaan.[26] Toisin kuin henkilötietolaissa, tietosuoja-asetuksessa ei ole säädetty rekisteröidyn suorittaman pyynnön määrämuotoisuudesta. Mikäli pyyntö on esitetty sellaisessa muodossa, joka antaa rekisterinpitäjälle perustellun syyn epäillä rekisteröidyn henkilöllisyyttä, voi rekisterinpitäjä pyytää rekisteröidyn henkilöllisyyden varmistamiseksi tältä tarvittavat lisätiedot.[27]

4.3 Oikeus tietojen oikaisemiseen sekä oikeus tulla unohdetuksi

Tietosuoja-asetuksessa, kuten myös henkilötietolaissa, on säädetty rekisteröidyn oikeudesta hänestä tallennettujen tietojen korjaamiseen. Rekisteröidyllä on myös sekä tietosuoja-asetuksen että henkilötietolain perusteella oikeus tallennettujen tietojen poistamiseen tietyin rajoituksin, eli oikeus tulla unohdetuksi, vaikka henkilötietolakiin ei tätä

[24] Hanninen ym. 2017, 57-59
[25] Autio ym. 2017, 23-24
[26] Henkilötietolaki 22.04.1999, 26 §
[27] Autio ym. 2017, 24-25

oikeutta olekaan kirjattu nimenomaisesti. Mikäli rekisteröity on pyytänyt rekisterinpitäjää poistamaan häntä koskevat tiedot, on rekisterinpitäjällä velvollisuus ilmoittaa tästä pyynnöstä myös niille kolmansille osapuolille, joilta tiedot on saatu tai joille niitä on luovutettu.[28]

Rekisteröidyllä on oikeus tietojen poistamiseen, jos tietojen säilyttäminen rikkoo tietosuoja-asetusta tai jäsenvaltion lainsäädäntöä. Tämä oikeus on voimassa myös silloin, jos henkilötietoja ei enää tarvita niihin käyttötarkoituksiin, joita varten ne on kerätty, tai jos rekisteröity on perunut tietojen käsittelyä koskevan suostumuksensa tai mikäli rekisteröity on vastustanut henkilötietojensä käsittelyä. Oikeus henkilötietojen poistamiseen rekisteristä tulee kyseeseen varsinkin silloin, kun rekisteröity on antanut suostumuksensa alaikäisenä ja haluaa myöhemmin poistaa nämä, erityisesti Internetissä saatavilla olevat tiedot. Rekisterinpitäjällä on pyynnöstä huolimatta oikeus jatkaa tietojen säilyttämistä ja käsittelyä, mikäli se on tarpeen jonkin lakisääteisen velvoitteen noudattamiseksi.[29]

4.4 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus rajoittaa henkilötietojen käsittelyä. Rajoitus voidaan toteuttaa esimerkiksi tietojen siirtämisellä toiseen järjestelmään tai estää käyttäjien pääsy valittuihin henkilötietohin. Tietojen käsittelyä koskeva rajoitus on pantava voimaan sellaisella tavalla, että henkilötiedot eivät enää myöhemmin päädy käsittelytoimenpiteiden kohteeksi. Rekisterinpitäjä saa edelleen säilyttää tietoja, mutta ei saa muulla tavoin käsitellä niitä ilman rekisteröidyn lupaa. Ennen kuin käsittelyn rajoitus poistetaan esimerkiksi rekisterinpitäjään kohdistuvan lakisääteisen velvoitteen toteuttamiseksi, tulee rekisteröityä informoida rajoituksen poistamisesta. Rekisteröidyllä on oikeus henkilötietojen käsittelyn rajoittamiseen, kun yksi seuraavista tietosuoja-asetuksen 18 artiklassa säädetyistä ehdoista täyttyy:[30]

a) Rekisteröity kiistää henkilötietojen paikkaansapitävyyden
b) Henkilötietojen käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista

[28] Autio ym. 2017, 25
[29] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 17. artikla
[30] Autio ym. 2017, 26

c) Rekisterinpitäjä ei enää tarvitse henkilötietoja aiemmin määritellyn käsittelyn tarkoituksiin
d) Rekisteröity on käyttänyt tietojen vastustamisoikeuttaan

4.5 Oikeus siirtää tiedot järjestelmästä toiseen

Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus siirtää itse toimittamansa henkilötiedot toiselle rekisterinpitäjälle nykyisen sitä hankaloittamatta. Rekisteröidyn tulee saada siirrettyä tiedot suoraan rekisterinpitäjien välillä, mikäli se on teknisesti mahdollista. Rekisteröidyn oikeus tietojen siirtoon on voimassa silloin, kun tietojen käsittelyyn on annettu suostumus tai sitä varten on tehty sopimus. Henkilötietojen käsittelyn tulee olla molemmissa edellä mainituissa tapauksissa automatisoitua.[31]

Tietosuojatyöryhmä WP29 on tuottanut ohjeistuksen, jossa avataan tarkemmin tietosuoja-asetuksen tietojen siirtämistä koskevaa sääntelyä. Ohjeistuksen mukaan rekisteröidyn itse toimittamiin henkilötietoihin sisältyy myös kaikki rekisteröidyn omalla toiminnallaan, kuten esimerkiksi jonkin palvelun tai laitteen käyttämisellä, generoima data. Esimerkkinä tästä generoidusta tiedosta voidaan mainita esimerkiksi haku- tai selailuhistoria tai paikannusdataa sisältävät tiedot. Jotta rekisterinpitäjän on helppo noudattaa tietosuoja-asetuksen ilmoitusvelvollisuutta, suosittelee tietosuojatyörymä rekisterinpitäjän ilmoittavan rekisteröidylle oikeudesta tietojen siirtoon aina ennen kunkin sopimuksen tai valtuutuksen purkautumista.[32]

4.6 Vastustamisoikeus

Kuten myös aikaisemmin mainitussa käsittelyn rajoittamisoikeudessa, on rekisteröidyllä oikeus vastustaa henkilötietojensa käsittelyä tietyissä, ennalta määritetyissä tilanteissa. Ne sisältävät käsittelyn suoramarkkinointia varten, sekä joissain tapauksissa myös historiallista, tieteellistä tai tilastollisia tutkimusta varten. Rekisteröity on oikeutettu vastustamaan tiedon käsittelyä myös silloin, kun kyseessä on yleistä etua koskevan tehtävän suorittaminen tai esimerkiksi rekisterinpitäjän oikeutetun edun toteuttaminen. Mikäli rekisteröity on käyttänyt vastustamisoikeuttaan, ei rekisterinpitäjä saa enää käsitellä tätä

[31] Autio ym. 2017, 26-27
[32] Guidelines on the right to data portability. 2016, 7-11

koskevia henkilötietoja. Rekisteröidyn on voitava käyttää vastustamisoikeuttaan automatisoidusti käyttämänsä palvelun teknisiä ominaisuuksia hyödyntäen, kun kyseessä ovat tietoyhteiskunnan palvelut.[33]

Rekisterinpitäjä voi rekisteröidyn vastustamisesta huolimatta jatkaa henkilötietojen käsittelyä, mikäli on osoitettavissa, että tietojen käsittelyyn on huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeudet, edut ja vapaudet tai jos se on tarpeen rekisterinpitäjän oikeusvaateen esittämiseksi, laatimiseksi tai puolustamiseksi.[34]

4.7 Automatisoituihin päätöksiin ja profilointiin liittyvät oikeudet

Tietosuoja-asetuksessa on kielletty tiettyjä poikkeustilanteita lukuunottamatta sellaiset automatisoidun tietojen käsittelyn avulla tehdyt päätökset, joilla on rekisteröityä koskevia oikeusvaikutuksia tai jotka muulla tavalla vaikuttavat rekisteröityyn merkittävästi. Edellä mainittuja poikkeuksia ovat sellaiset tapaukset, joissa tehty päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä varten tai jos päätös perustuu rekisteröidyn nimenomaiseen suostumukseen. Nämä automatisoidut päätökset ja henkilötietojen profilointi eivät kuitenkaan saa perustua erityisiin henkilötietoryhmiin, paitsi edellä mainituissa poikkeustapauksissa ja mikäli toimenpiteet rekisteröidyn oikeuksien suojaamiseksi on toteutettu.[35]

[33] Autio ym. 2017, 27
[34] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 21. artikla
[35] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 22. artikla

5 TIETOSUOJAVASTAAVA

5.1 Tietosuojavastaavan nimittäminen

Rekisterinpitäjän ja henkilötietoja käsittelevän organisaation tulee tietosuoja-asetuksen mukaan nimittää tiettyjen organisaatiota koskevien vaatimusten täyttyessä tietosuojavastaava, joka valvoo tietosuoja-asetuksen noudattamista henkilötietojen käsittelyssä. Tietosuojavastaava on nimitettävä, kun yrityksen toiminnan ydintehtävät edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmälistä seurantaa tai jos ydintehtävät muodostuvat lajaamittaisesta arkaluontoisten henkilötietojen käsittelystä. Ydintehtävillä tarkoitetaan organisaation avaintoimintoja, joita edellytetään rekisterinpitäjän tai henkilötietojen käsittelijän tavoitteiden saavuttamiseksi. Avaintoimintoja voivat olla esimerkiksi potilaskertomusten tai muiden terveystietojen käsittely sairaalassa tai vakuutusyhtiön tekemän vastuunvalinnan yhteydessä. Tietosuojavastaavan yhteystiedot on julkistettava ja ne on ilmoitettava myös valvontaviranomaiselle. Tietosuojavastaavan on oltava helposti tavoitettavissa, eli käytännössä yrityksen on ilmoitettava vähintään tietosuojavastaavan osoite, puhelinnumero ja sähköpostiosoite.[36]

Tietosuojavastaava voidaan nimittää yrityksen omasta henkilöstöstä tai tehtävä voidaan tarvittaessa ulkoistaa myös organisaation ulkopuolelta tulevalle henkilölle. Huomioon on kuitenkin otettava henkilön pätevyys sekä asiaan liittyvän lainsäädännön tuntemus, jotta valittu henkilö pystyy selviytymään tehtävästään. Tietosuojavastaavan on oltava riippumaton, joten tehtävään ei voida valita sellaisia henkilöitä, jotka esimerkiksi vastaavat yrityksen tietojärjestelmistä tai päättävät henkilötietojen käyttötarkoituksesta yrityksessä.[37]

5.2 Tietosuojavastaavan asema

Tietosuoja-asetuksen mukaan organisaation tietosuojavastaava on otettava mukaan kaikkien henkilötietojen suojaa koskettavien kysymysten käsittelyyn ja tietosuojavastaavaa on myös tuettava tehtävän suorittamiseen sekä kouluttautumiseen vaadittavilla resursseilla. Tietosuojavastaava ei saa ottaa vastaan ohjeita tehtävien suorittamiseen liittyen, vaan tehtävään nimetyn henkilön tulee selvitä näistä itsenäisesti. Rekisterinpitäjä

[36] Tietosuojavaltuutetun verkkosivut. 2017
[37] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 37. artikla

tai henkilötietoja käsittelevä organisaatio ei saa rangaista tai erottaa tietosuojavastaavaa sen vuoksi, että tämä on hoitanut tehtäviään. Rekisteröityjen on voitava ottaa yhteyttä tietosuojavastaavaan kaikissa omien henkilötietojensa käsittelyyn tai tietosuoja-asetukseen perustuvien oikeuksiensa käyttöön liittyvissä asioissa. Tietosuojavastaavan on voitava suorittaa myös muita tehtäviä ja velvollisuuksia, mutta niiden suorittaminen ei saa aiheuttaa eturistiriitoja tietosuojavastaavan tehtävien kanssa.[38]

5.3 Tietosuojavastaavan tehtävät

Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietoja käsittelevän organisaation ylimmälle johdolle. Hän ei kuitenkaan osallistu itse päätöksentekoon, vaan hänen tulisi toimia konsultin ominaisuudessa opastaen ja antaen neuvoa henkilöstölle liittyen tietosuoja-asetuksen sekä muiden organisaatiota sitovien tietosuojasäännösten mukaisiin velvollisuuksiin. Hänen tulee myös seurata tietosuoja-asetuksen sekä muun tietosuojalainsäädännön noudattamista organisaation sisällä. Käytännössä tämä tapahtuu tiedon lisäämisellä sekä henkilöstön koulutuksiin tai niiden suunnitteluun osallistumisella. Tietosuojavastaavan on tehtävä yhteistyötä valvontaviranomaisen kanssa ja hänen on samalla toimittava yhteyshenkilönä rekisteröityjen sekä organisaation ja valvontaviranomaisen välillä, salassapitovelvollisuuden sitomana. Tehtäviä suorittaessaan tietosuojavastaavan on otettava huomioon henkilötietojen käsittelytoimiin liittyvä riski suhteutettuna käsittelyn luonteeseen, laajuuteen ja tarkoitukseen.[39]

[38] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 38. artikla
[39] Hanninen ym. 2017, 121-123

6 SELOSTE KÄSITTELYTOIMISTA

Tietosuoja-asetuksen mukaan jokaisen yli 250 henkilöä työllistävän rekisterinpitäjän ja tarvittaessa myös sen edustajan on ylläpidettävä kirjallista, myös sähköisessä muodossa saatavilla olevaa selostetta sen henkilötietoja koskettavista käsittelytoimista. Ylläpitovelvollisuus koskee myös edellä mainittua pienempää rekisterinpitäjää, mikäli sen suorittama henkilötietojen käsittely voi todennäköisesti aiheuttaa riskin rekisteröidyn vapauksille ja oikeuksille, sen suorittama henkilötietojen käsittely ei ole satunnaista tai niiden käsittely kohdistuu erikseen mainittuihin erityisiin tietoryhmiin tai sellasiin tietoihin, jotka koskevat rikostuomioita tai rikkomuksia. Seloste käsittelytoimista tulee sisältää vähintään kaikki seuraavat tiedot:[40]

a) Rekisterinpitäjän ja tarvittaessa myös sen edustajan nimi, osoite, sekä tietosuojavastaavan yhteystiedot
b) Tietojen käsittelyn tarkoitus
c) Kuvaus rekisteröityjen ryhmistä
d) Kuvaus henkilötietoryhmistä
e) Ne tahot, joille henkilötietoja on luovutettu tai voidaan luovuttaa
f) Tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
g) Mahdollisuuksien mukaan tietoryhmien poistamisen määräajat
h) Kuvaus niistä teknisistä ja organisatorisista toimista, jotka rekisterinpitäjä on tehnyt henkilötietojen suojaamiseksi

Seloste käsittelytoimista on organisaation sisäinen asiakirja eikä sitä ole tarkoitettu käytettäväksi suoraan rekisteröityjen informoitiin, vaikka sen sisältöä voidaan helposti hyödyntää edellä mainitussa tapauksessa.[41]

[40] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 30. artikla
[41] Tietosuojavaltuutetun verkkosivut. 2017

7 SANKTIOT

7.1 Sanktion määrääminen

Tietosuoja-asetuksen rikkomisesta voidaan määrätä hyvin ankaria hallinnollisia sakkoja. Valvontaviranomaisten on kuitenkin varmistettava, että niden määrääminen on kussakin yksittäisessä tapauksessa varoittavaa, oikeasuhteista ja tehokasta. Sakko voidaan määrätä tapauskohtaisesti valvontaviranomaisen suorittamien korjaavien toimenpiteiden lisäksi tai niiden sijasta. Hallinnollisen sakon määräämiseen ja sen määrään vaikuttavat rikkeen vakavuus, laajuus ja tuottamuksellisuus. Rikettä lieventäviä asioita voivat olla rekisterinpitäjän tai henkilötietojen käsittelijän suorittamat ehkäisevät toimenpiteet sekä yhteistyö valvontaviranomaisen kanssa. Raskauttavina asioina voidaan taas pitää aiempia vastaavia rikkomuksia, rikkeestä mahdollisesti aiheutunutta taloudellista hyötyä sekä rikkeen kohdistumista erityisiin henkilötietoryhmiin.[42]

7.2 Sanktion määrä

Määrättävän sakon enimmäismäärän suuruus riippuu siitä, minkä säännöksen rikkominen on kyseessä. Mikäli rekisterinpitäjä tai henkilötietojen käsitelijä rikkoo samalla kertaa tai toisiinsa liittyvissä käsittelytoimissa useampaa kuin yhtä säännöstä, saa määrättävän sakon kokonaismäärä olla enintään vakavimmasta rikkomuksesta määrätyn sakon suuruinen. Sakko voidaan määrätä kahdesta eri suuruusluokasta rikotuista säännöksistä riippuen.[42]

Pienempi hallinnollinen sakko on määrältään enintään 10 000 000 euroa, tai mikäli kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden kokonaisliikevaihdosta sen mukaan, kumpi edellä mainituista summista on suurempi. Pienempi sakko voidaan määrätä, kun rikkomus on kohdistunut seuraaviin säännöksiin: [42]

a) 8 artiklassa säädettyyn lapsen suostumukseen sovellettaviin ehtoihin
b) 11 artiklassa säädettyyn käsittelyyn, joka ei edellytä tunnistamista

[42]Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 83. artikla

c) 25-39 artiklassa säädettyihin rekisterinpitäjän ja henkilötietojen käsittelijän yleisiin velvollisuuksiin, henkilötietojen tietosuojaan sekä tietosuojavastaavan toimintaan
d) 42 ja 43 artiklassa säädettyihin sertifiointiin liittyvät velvollisuudet

Suurempi hallinnollinen sakko on määrältään enintään 20 000 000 euroa, tai mikäli kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden kokonaisliikevaihdosta sen mukaan, kumpi edellä mainituista summista on suurempi. Suurempi sakko voidaan määrätä, kun rikkomus on kohdistunut seuraaviin säännöksiin:[43]

a) 5-7 ja 9 artiklassa säädettyihin käsittelyn perusperiaatteisiin
b) 12-22 artiklassa säädettyihin rekisteröidyn oikeuksiin
c) 44-49 artiklassa säädettyyn henkilötietojen siirtoon kolmansiin maihin tai kansainvälisille järjestestöille
d) 85-91 artiklassa säädettyjen tietojenkäsittelyyn liittyvien erityistilanteita koskeviin säännöksiin
e) Valvontaviranomaisen 58 artiklan nojalla antaman määräyksen tai rajoituksen noudattaminen tai valvontaviranomaisen tietoihin pääsyn antamista koskeva velvollisuus

Julkishallinnon elimien ja viranomaisten kohdalla jokainen jäsenvaltio voi asettaa omia sääntöjä siitä, voidaanko näille tahoille määrätä kyseisessä valtiossa hallinnollisia sakkoja ja missä määrin. Nämä säännöt eivät kuitenkaan saa rajoittaa 58 artiklan mukaisia valvontaviranomaisen korjaavia toimivaltuuksia. Mikäli jäsenvaltion oikeusjärjestelmissä ei ole säädetty hallinnollisista sakoista, voidaan tietosuoja-asetusta soveltaa siten, että sakon panee vireille jokin muu toimivaltainen valvontaviranomainen ja sen määräävät kansalliset tuomioistuimet. Samalla on varmistettava, että määrättävät sanktiot ovat yhtä lailla tehokkaita, oikeasuhtaisia ja tehokkaita, kuin valvontaviranomaisten määräämillä hallinnollisilla sakoilla.[43]

[43] Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, 83. artikla

8 UUSI TÄSMENTÄVÄ TIETOSUOJALAKI

Vaikka tietosuoja-asetus onkin kansallisesti suoraan sovellettava säädös, on EU:n jäsenvaltioiden mahdollista täydentää, täsmentää tai soveltaa sitä omalla lainsäädännöllä. Suomessa tämä on esitetty toteutettavan uuden tietosuojalain säätämisellä. Tietosuojalain on tarkoitus toimia henkilötietojen käsittelyä koskevana yleislakina. Sen täytäntöönpano on lähtenyt liikkeelle hallituksen eduskunnalle 1.3.2018 antamasta esityksestä HE 9/2018. Tämän opinnäytetyön kirjoittamishetkellä toinen eduskunnan tietosuojalakia koskeva käsittely on saatu päätökseen 13.11.2018. Eduskunta on käsittelyssään hyväksynyt hallituksen esityksessä esitetyn uuden tietosuojalain hallintovaliokunnan mietinnön mukaisesti.[44]

Hallituksen hyväksymä 1. lakiehdotus käsittää itse tietosuojalain säännökset. Hyväksytyt lakiehdotukset 2-4 käsittävät jo olemassaoleviin lakeihin tehtävät muutokset tai lisäykset, joissa huomioidaan yleinen tietosuoja-asetus sekä tietosuojalaki. Nämä sisältävät muutoksia rikoslain 38 luvun tietosuojarikoksia ja syyteoikeutta koskeviin 9 ja 10 §:ään, sakon täytäntöönpanosta annetun lain 1 §:ään sekä harmaan talouden selvitysyksiköstä annetun lain 12 §:ään.[45]

Tietosuojalaissa on säädetty tarkemmin esimerkiksi kansallisen valvontaviranomaisen kelpoisuusvaatimuksista, tietojenkäsittelyn erityistilanteista sekä uhkasakoista ja hallinnollisista seuraamusmaksuista. Siinä on tarkennettu muun muassa henkilötietojen käsittelyn lainmukaisuutta tietyissä yleisissä tapauksissa. Esimerkkinä voidaan mainita sellaiset tilanteet, joissa tietosuoja-asetuksen 9 artiklan 1 kohdassa määriteltyä erityisten henkilötietoryhmien käsittelyn kieltoa ei sovelleta. Näihin tilanteisiin lukeutuu esimerkiksi sellainen vakuutusyhtiöiden suorittama henkilötietojen käsittely, joka koskettaa vakuutustoiminnassa saatuja tietoja vakuutetun tai korvauksenhakijan terveydentilasta, häneen kohdistetuista hoitotoimenpiteistä tai muista toimista, jotka ovat tarpeen vakuutusyhtiön vastuun selvittämiseksi.[45]

[44] Eduskunnan verkkosivut. 2018.
[45] Hallituksen esitys HE 9/2018

9 TYÖN TAVOITTEET JA TUTKIMUSKYSYMYKSET

Tämän opinnäytetyön tavoitteena on selventää tietosuoja-asetusta ja esittää henkilötietoja käsittelevän ja henkilörekisteriä ylläpitävän organisaation kannalta tärkeimpiä huomioon otettavia seikkoja helposti ymmärrettävässä ja tiiviissä muodossa. Erityisesti huomioon on pyritty ottamaan sellaisen yrityksen näkökulma, jossa henkilötietojen käsittely kuuluu yrityksen jokapäiväiseen toimintaan. Tarkoituksena on, että yritys, rekisterinpitäjä tai näiden edustaja pystyy tämän työn avulla poimimaan tietosuoja-asetuksesta ne tärkeimmät asiat, joihin yrityksen tulisi kiinnittää huomiota tulevaisuudessa, jotta kyseessä olevan organisaation henkilötietojen käsittely olisi toteutettu asetuksen edellyttämällä tavalla.

Opinnäytetyössä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

1. Mikä on tietosuoja-asetuksen tarkoitus?
2. Mitkä ovat tärkeimmät tietosuoja-asetuksen säännökset?
3. Mitä toimenpiteitä yrityksen tulee tehdä ja mitä asioita sen tulisi ottaa huomioon, jotta sen suorittama henkilötietojen käsittely on toteutettu asetuksen vaatimalla tavalla?

10 JOHTOPÄÄTÖKSET JA POHDINTA

Tietosuoja-asetuksen täytäntöönpano on aiheuttanut niin pienille kuin suurille organisaatioille paljon lisätyötä, jotta ne ovat pystyneet tarvittaessa muokkaamaan prosessejaan, järjestelmiään ja toimintatapojaan vastamaan tietosuoja-asetuksen mukanaan tuomiin vaatimuksiin annetun siirtymäajan puitteissa. Se sisältää yrityksiä ja yhteisöjä koskevien säännösten lisäksi myös paljon vain julkishallintoa tai viranomaisia koskevia säännöksiä, joten oleellisen ja tärkeän tiedon poiminta, sekä asetuksen tulkinta yleensä, voi olla hankalaa. Tästä syystä on erityisen tärkeää, että organisaation tietosuojavastaava on tutustunut huolella asetuksen sisältöön ja tuntee myös muuta asiaan liittyvää lainsäädäntöä tai sääntelyä sen lisäksi. Tällä tavoin organisaation johto pystyy varmistumaan siitä, että kaikki tarvittavat asiat on otettu huomioon ja että organisaation tietosuoja on vähintäänkin riittävän hyvällä tasolla.

Tietosuoja-asetuksessa painotetaan rekisteröidyn oikeuksia ja sitä, että nämä oikeudet myös tuodaan heidän tietoonsa selkällä ja ymmärrettävällä tavalla. Rekisteröidyn on erityisesti oltava tietoinen siitä, miten ja mihin hänen henkilötietojaan käytetään sekä kenelle niitä jaetaan. Toinen painopiste on rekisterinpitäjän sekä henkilötietojen käsittelijän velvollisuuksista kiinni pitäminen, vaikka toki myös rekisterinpitäjän on hyvä olla tietoinen myös omista oikeuksistaan tätä sitovien velvollisuuksien lisäksi. Kolmas tärkeä asia asetuksessa on kaiken organisaation suorittaman henkilötietojen käsittelyn lain- ja tarkoituksenmukaisuuden varmistaminen, unohtamatta henkilötietojen säilytysajan rajoittamista vain sellaiseen ajanjaksoon, joka on tarkoituksenmukaista kyseessä olevien henkilötietojen käsittelemistä varten.

Vaikka tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselosteen ylläpitoa, rekisterinpitäjän on kuitenkin hyvä panostaa selosteen tai selosteiden valmisteluun ja niissä olevan tiedon määrään. Edellä mainitut kirjalliset kuvaukset ovat yksinkertainen, selkeä, helppo ja rekisteröidyn kannalta kannalta hyvä tapa täyttää osa rekisterinpitäjän tiedonantovelvollisuudesta organisaation suorittamaan henkilötietojen käsittelyyn liittyen. Tiedonantovelvollisuuden täyttymistä edesauttaa merkittävästi, jos iso määrä siitä tiedosta, joka rekisteröidylle pitää tuoda julki esimerkiksi jonkin sopimuksen tekovaiheessa, on jo luettavissa suoraan julkisesta rekisteri- tai tietosuojaselosteesta. Rekisterinpitäjän ja organisaation tietosuojavastaavan työtä selosteen valmistelun suhteen helpottaa se seikka, että erittäin suuri osa suomalaisten yritysten rekisteri- ja

tietosuojaselosteista on luettavissa näiden verkkosivuilla digitaalisessa muodossa. Valmiista selosteista on helppo tutkia, mitä tietoja niissä on mahdollista ilmoittaa tietosuoja-asetuksessa lueteltujen pakollisten tietojen lisäksi ja missä muodossa nämä pakolliset tiedot on ilmoitettu käytännössä.

Organisaation hallussa olevat henkilötiedot tulee säilyttää sellaisessa muodossa, ettei ulkopuolinen taho pääse niihin luvatta käsiksi tai saa selville niiden sisältöä tai ketä ne koskevat. Käytännössä tämä edellyttää tietyn tasoista tietojen suojausta tai salausta, henkilötietotyypeistä ja rekisterinpitäjän käytössä olevista järjestelmistä riippuen. Organisaation on näin ollen taattava käytössä olevien järjestelmien toimintavarmuus ja vikasietoisuus. Erityisen tärkeää on mahdollistaa nopea ja helppo tietojen palautus mahdollisesta vikatilanteesta tai tietoturvaloukkauksesta johtuvan tietojen katoamisen takia. Tällä tavoin voidaan minimoida vikatilanteen tai tietoturvaloukkauksen vaikutus yrityksen toimintaan ja edesauttaa organisaation normaalin toiminnan jatkumista tapahtuneesta huolimatta.

Tietosuoja-asetuksen rikkomisesta mahdollisesti määrättävät hallinnolliset sakot ovat suuruusluokaltaan valtavan isoja. Niiden on kuitenkin tarkoitus lähinnä toimia pelotteena ja niin sanotusti ohjata yritykset ottamaan paremmin huomioon henkilötietojen suojan toiminnassaan. Sakoista on säädetty erityisesti isot monikansalliset digialan yritykset silmällä pitäen. Näitä sakkoja tuskin tullaan määräämään helposti täysimääräisenä, sillä se käytännössä vaatisi tahallisuutta, törkeää huolimattomuutta ja yhteistyöstä kieltäytymistä valvontaviranomaisen kanssa. Tämän työn kirjoittamishetkellä ei ole vielä tiedossa yhtään tapausta, joiden pohjalta yrityksille olisi määrätty sakkoja. Isoista yrityksistä kuitenkin muun muassa Facebookista, Amazonista ja Googlesta on heti siirtymäajan päättymisen jälkeen tehty useampia kanteluita tietosuoja-asetuksen rikkomisen takia.[46] Edellä mainitut yritykset ovat kuitenkin niin suuria, että asian tutkiminen ja käsittely tulee viemään hyvin paljon aikaa, sillä läpi käytävän datan määrä on massiivinen. Käytännössä mahdollisista päätöksistä tullaan kuulemaan vasta kuukausien tai jopa vuosien päästä.

Tietosuoja-asetus on pohjimmiltaan säädetty parantamaan ihmisten luottamusta verkosta löytyviin palveluntarjoajiin, niiden suorittamaan henkilötietojen käsittelyyn sekä helpottamaan digitaalisten palveluiden tarjoamista yli kansallisten rajojen. Yritysten kannattaa tämän perusteella ottaa asetuksen mukanaan tuomat haasteet ja muutokset vastaan postiviisin mielin, sillä prosessien läpinäkyvyyden lisäämisen takia asetuksen

[46] ZDNet.com verkkosivut. 2018

voimaantulolla tulee todennäköisesti olemaan hyvin paljon enemmän positiivisia kuin negatiivisia vaikutuksia yritysten toimintaan.

LÄHTEET

Andreasson A., Riikonen J. & Ylipartanen A. 2017. Osaava tietosuojavastaava. Tallinna: Printon.

Article 29 Data Protection Working Party. 2016. Guidelines on the right to data portability. Viitattu 23.04.2018. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Autio E., Hänninen A., Kantonen S., Pihamaa H-T. & Talus A. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Helsinki: Oikeusministeriö ja tietosuojavaltuutetun toimisto. Viitattu 11.04.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf.

Eduskunnan verkkosivut 2018. EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano – Uusi tietosuojalaki. Viitattu 12.11.2018. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx

Elisa, Suomen Yrittäjät & Prior Konsultointi. 2016. Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten PK-yritysten digitalisaation asteesta. Viitattu 02.05.2018. Ladattavissa: https://hub.elisa.fi/digitaalisuuden-hyodyntamisella-merkittava-yhteys-pk-yritysten-menestykseen/

Enroth T. & Neuvonen R. 2017. EU:n tietosuoja-asetuksen yritysvaikutukset. Valtioneuvoston selvitys- ja tutkimustoiminnan artikkelisarja. Viitattu 02.05.2018. http://tietokayttoon.fi/documents/1927382/2116852/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset/

Euroopan parlamentin ja neuvoston asetus (EU) 679/2016. Annettu Brysselissä 27.04.2016. Saatavilla sähköisesti osoitteessa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Hallituksen esitys HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Annettu Helsingissä 1.3.2018. Saatavilla sähköisesti osoitteessa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

Hanninen M., Laine E., Rantala M., Rusi M & Varhela M. 2017. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Vantaa: Helsingin Kamari Oy.

Henkilötietolaki 523/1999. Annettu Helsingissä 22.04.1999. Saatavilla sähköisesti osoitteessa: https://www.finlex.fi/fi/laki/ajantasa/1999/19990523.

Savon Sanomat 22.06.2017. https://www.savonsanomat.fi/kotimaa/Petossarjassa-k%C3%A4ytettiin-vuonna-2011-vuodettuja-tietoja-%E2%80%93-murtoja-tehty-my%C3%B6s-It%C3%A4-Suomen-yliopiston-tietokantoihin/1005735. Viitattu 24.04.2018.

Tietosuojavaltuutetun verkkosivut 2017. Tietosuojavastaavat. Viitattu 11.04.2018. http://www.tietosuoja.fi > EU:n tietosuojauudistus > Ohjeita > Tietosuojavastaavat

Tietosuojavaltuutetun verkkosivut 2018. Henkilötietolaki. Viitattu 20.10.2018. http://www.tietosuoja.fi > Tietosuoja > Lainsäädäntöä > Henkilötietolaki

Tivi 24.04.2018. https://www.tivi.fi/Kaikki_uutiset/tietomurto-matkailuyhtion-jarjestelmiin-myos-suomalaisten-maksukorttitietoja-vaarassa-6721859. Viitattu 24.04.2018.

Yle 09.04.2018. https://yle.fi/uutiset/3-10150705. Viitattu 24.04.2018.

ZDNet.com verkkosivut 2018. GDPR attacks: First Google, Facebook, now activists go after Apple, Amazon, LinkedIn. Viitattu 20.10.2018. https://www.zdnet.com/article/gdpr-attacks-first-google-facebook-now-activists-go-after-apple-amazon-linkedin