Ville Kotro

YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET ORGANISAATIOIDEN DATAN KÄSITTELYYN SEKÄ SEN KUSTANNUSVAIKUTUKSET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Kotro, Ville
YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET ORGANISAATIOIDEN DATAN KÄSITTELYYN SEKÄ SEN KUSTANNUSVAIKUTUKSET
Jyväskylä: Jyväskylän yliopisto, 2023, 23 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Kyppö, Jorma

Digitalisoituneessa yhteiskunnassa kansalaisista syntyy jatkuvasti valtava määrä dataa. Tämän datan perusteella ihmisiä voidaan usein yksilöidä ja se on myös erilaisille yrityksille arvokasta. Tietojenkäsittelyä, etenkin henkilötietojen osalta, on säädelty laeilla jo pitkään, mutta kiihtyvä digitalisaatio on asettanut uudenlaisia haasteita. Euroopan unionin yleisellä tietosuoja-asetuksella (GDPR) pyritään varmistamaan kansalaisten oikeuksien toteutuminen digimaailmassa sekä yhtenäistämään lainsäädäntöä unionin alueella. GDPR uudisti tietojenkäsittelyyn liittyvää lainsäädäntöä melko mittavasti, joten yritysten on täytynyt tehdä monenlaisia uudistuksia saadakseen toimintansa vastaamaan asetuksen vaatimuksia.

Tämän kandidaatintutkielman tarkoituksena on selvittää, kuinka Euroopan unionin yleisen tietosuoja-asetuksen asettamiin vaatimuksiin on vastattu yrityksissä. Erityisesti tutkielmassa on keskitytty datan hallinnan muutoksiin yrityksissä ja asetuksen aiheuttamiin kustannuksiin, sekä sen vaikutukseen yritysten kilpailukykyyn. Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena, ja siinä tutkittiin useiden aiempien tutkimusten tuloksia ja luotiin näistä synteesi. GDPR:n vaikutukset yrityksille ovat olleet erilaisia riippuen esimerkiksi organisaatioiden toimialasta ja koosta. Vaikutukset ovat olleet suurimpia pk-yrityksille. Lisäksi tietointensiivisen teknologiasektorin yritykset ovat joutuneet muuttamaan prosessejaan enemmän verrattuna perinteisen teollisuuden yrityksiin.

Asiasanat: Yleinen tietosuoja-asetus, GDPR, datan hallinta, tietosuoja, kustannusvaikutus, kilpailukyky

ABSTRACT

Kotro, Ville
IMPACTS OF THE GENERAL DATA PROTECTION REGULATION (GDPR) ON ORGANIZATIONS' DATA PROCESSING AND ITS COST IMPLICATIONS.
Jyväskylä: University of Jyväskylä, 2023, 23 pp.
Information Systems, Bachelor's thesis
Supervisor: Kyppö, Jorma

In a digitized society, a tremendous amount of data is constantly generated by citizens. Based on this data, individuals can often be identified, and it is also valuable to various companies. Data processing, especially concerning personal data, has long been regulated by laws, but the accelerating digitalization has posed new challenges. The General Data Protection Regulation (GDPR) of the European Union aims to ensure the realization of citizens' rights in the digital world and harmonize legislation within the Union's territory. GDPR has significantly revised the legislation related to data processing, requiring companies to make various reforms to align their operations with the requirements set by the regulation.

The purpose of this bachelor's thesis is to investigate how businesses have responded to the requirements set by the General Data Protection Regulation of the European Union. Specifically, the research focuses on changes in data management within companies, the costs incurred due to the regulation, and its impact on the competitiveness of businesses. The thesis was conducted as a systematic literature review, examining the results of several previous studies and synthesizing them. The impacts of GDPR on companies have varied, depending on factors such as the industry and size of organizations. The impacts have been most significant for small and medium-sized enterprises (SMEs). Additionally, companies in the information-intensive technology sector have had to modify their processes to a greater extent compared to traditional industrial companies.

Keywords: General Data Protection Regulation, GDPR, data management, data protection, cost impact, competitiveness

SISÄLLYS

1 Johdanto

Digitalisoituvassa yhteiskunnassa ihmisistä kertyy jatkuvasti enemmän tietoa verkkoon. Jokaisen kansalaisen oikeus omiin henkilötietoihin on suojattu jo Euroopan unionin perusoikeuskirjassa. Useille yrityksille käyttäjien tiedot ovat myös liiketoiminnan ydin. Henkilötiedot ovat arvokasta omaisuutta myös muille yrityksille, koska tietojen avulla mm. kehitetään liiketoimintaa entistä asiakaslähtöisemmäksi ja kohdennetaan markkinointitoimenpiteitä. Aikaisempi EU:n tietosuojadirektiivi säädettiin vuonna 1995, minkä jälkeen internet ja siellä oleva tietomäärä on kasvanut valtaisasti. Kansalaisten henkilötietojen suojaamiseksi ryhdyttiin kehittämään uutta tietosuojalainsäädäntöä 2010-luvun alussa. (Euroopan komission verkkosivut, 2022)

Tämän kandidaatintutkielman tarkoituksena on selvittää, kuinka Euroopan Unionin yleinen tietosuoja-asetus on vaikuttanut yritysten henkilötietojen keräämiseen ja hallintaan, niiden tietojärjestelmiin sekä tutkia millaisia kustannusvaikutuksia uusi lainsäädäntö on aiheuttanut yrityksille.

Tämän kandidaatintutkielman tutkimusmenetelmäksi valikoitui systemaattinen kirjallisuuskatsaus. Systemaattisella kirjallisuuskatsauksella saadaan muodostettua tiivis kuva laajoista tietomääristä. Katsauksessa kerätään ensin tietoa hyviksi tunnistetuista lähteistä, arvioidaan tutkimusten relevanssia aiheeseen sekä yhdistellään kirjallisuuden tuloksista synteesi. Tavoitteena systemaattisessa kirjallisuuskatsauksessa on tiivistää aiempien tutkimusten tuloksia ja muodostaa niistä kokonaisuus, joka vastaa kirjallisuuskatsauksen tutkimuskysymyksiin. (Petticrew, 2001)

Systemaattisen kirjallisuuskatsauksen kuvaamiseksi on olemassa seitsenosainen Finkin-malli. Malli selventää katsauksen tekemistä aina tutkimuskysymysten asettamisesta tulosten analysointiin. Ensin systemaattisessa kirjallisuuskatsauksessa tulee valita tutkimuskysymykset, joihin kirjallisuuskatsauksella halutaan löytää vastauksia. Tässä kandidaatin tutkielmassa tutkimuskysymykset ovat:

- Millaisia vaikutuksia GDPR:llä on ollut yritysten datan hallintaan?

- Millaisia kustannusvaikutuksia GDPR:llä on ollut organisaatioille?

Kirjallisuuskatsauksen toisessa vaiheessa valitaan kirjallisuuden etsimiseen käytettävät tietokannat. Tässä työssä lähteet on etsitty Google Scholar- ja JYKDOK-tietokannoista. Tietokantavalintojen jälkeen kolmannessa vaiheessa valitaan hakusanat ja -lauseet, joilla tietoa kannoista etsitään. Sopivasti valikoidut hakusanat rajaavat tarpeettomat tulokset pois ja tiedon määrä pysyy hahmotettavana. Tätä kirjallisuuskatsausta varten käytettyjä hakutermejä ovat: general data protection regulation, data protection, effects, firms, companies, tietosuoja, tietosuoja-asetus, vaikutus ja personal data. Hauissa hyödynnettiin myös loogisia operaattoreita AND ja OR.

Neljännessä vaiheessa seulotaan tuloksia esimerkiksi materiaalin julkaisukielen ja -ajankohdan perusteella. Tähän kandidaatintutkielmaan valikoitui suomen- ja englanninkielisiä lähteitä, jotka on julkaistu 2010- tai 2020-luvulla. Viidennessä vaiheessa lähteitä suodatetaan metodologisesta näkökulmasta, eli arvioidaan kirjallisuuden tieteellistä luotettavuutta ja laatua. Tässä on pyritty huomioimaan kirjallisuuden vertaisarviointi, niihin tehtyjen viittausten määrä sekä alusta, jolla kirjallisuus on julkaistu. Seuraavaksi systemaattisessa kirjallisuuskatsauksessa muodostetaan itse katsaus. Katsauksen tulokset ja niistä koostettu kuva on esitelty tämän tutkielman osalta luvuissa 3.1., 3.2. ja 3.3. (Salminen, 2011).

Tutkielman lopussa kootaan tuloksia yhteen. Luvussa 4 arvioidaan aiheen tulevaisuuden näkymiä ja tarjotaan mahdollisia jatkotutkimuskohteita.

2 Yleinen tietosuoja-asetus, henkilötieto ja tietosuoja

2.1 Henkilötieto

Euroopan Unionin yleisen tietosuoja-asetuksen määritelmän mukaan henkilötieto on mikä tahansa sellainen tieto, jolla voidaan yksilöivästi tunnistaa luonnollinen henkilö, josta tietoja on tallennettu. Tällaisia tietoja ovat esimerkiksi nimi, osoite, puhelinnumerot, henkilökortin numero, paikannustiedot ja IP-osoite, sekä isovanhempien perinnölliset sairaudet. Henkilöä, jonka henkilötietoja on tallennettu, kutsutaan rekisteröidyksi. Mikäli tiedot anonymisoidaan esimerkiksi tutkimuksen aineistossa, eivät nämä silloin ole henkilötietoja. (tietosuoja.fi, 2022)

Yritykset ja muut organisaatiot voivat haluta kerätä käyttäjiensä henkilötietoja monista syistä. Esimerkiksi monien tietotalouden yritysten koko liiketoiminta perustuu tietojen keräämiseen ja myymiseen. Organisaatioilla on monia keinoja henkilötietojen keräämiseen käyttäjiltä. Käyttäjä voi antaa dataa vapaaehtoisesti ja asiaa sen suuremmin miettimättä, esimerkiksi lataamalla kuvia ja videoita sosiaalisen median palveluihin, kuten Facebookiin tai Instagramiin. Toiseksi yritykset voivat hankkia näitä yksilöiviä tietoja käyttäjien laitteilta, kuten esimerkiksi seuraamalla Google-hakuja. Näitä tietoja annetaan organisaatiolle yleensä tietämättä ja ilman suostumusta. Henkilöllä itsellään ei tällaisissa tilanteissa ole aikaisemmin ollut juuri valtaa vaikuttaa näin kerättyihin tietoihin. Kolmas tapa kerätä henkilötietoja on järjestelmien käyttäjänsä puolesta käsittelemästä datasta**.** Järjestelmät käsittelevät usein henkilöön liittyvää raakadataa merkitykselliseksi tiedoksi luomalla automaattisesti esimerkiksi analytiikkaa ja tilastoja käyttäjistä. (Pangrazio & Selwyn, 2018)

2.2 Tietosuoja

Tietosuojavaltuutetun verkkosivujen mukaan tietosuoja on henkilön perusoikeus, jolla turvataan rekisteröidyn oikeuksien toteutuminen, kun henkilötietoja käsitellään. Tietosuojan tehtävä on määritellä, millä oikeuksilla käsittely tapahtuu (tietosuoja.fi, 2022).

Pleger, Guirguis ja Mertes (2021) kuvaavat artikkelissaan tietosuojaa kolmesta näkökulmasta. Tietosuojaan on lainopillinen-, subjektiivinen- ja tekninen näkökulma. Ihmisten tietosuojaa varmistetaan erilaisilla laeilla ja asetuksilla, kuten tämän tutkielman aiheena olevalla Yleisellä tietosuoja-asetuksella. Usein näillä laeilla ja asetuksilla suojataan myös kansalaisten yksityisyyttä, joka on läheisessä yhteydessä tietosuojaan. Tietosuojaa ja yksityisyyttä käytetään usein samoissa yhteyksissä, mutta tietosuojan voidaan ajatella turvaavan oikeuksia laajemmin. Esimerkiksi tietosuojan ollessa kunnossa, kansalaisella pitää olla oikeus

päättää omien tietojensa käytöstä verrattuna siihen, että ne vain pidetään muilta piilossa. Tekninen näkökulma tietosuojaan käsittää tekniset ratkaisut, joilla tiedot pidetään turvassa. Tekniset ratkaisut varmistavat, että lain määräykset toteutuvat. Esimerkiksi järjestelmiä kehittäessä, tulee lait ja asetukset huomioida jo alusta alkaen. Tietosuojan kannalta hyvät ratkaisut tulee toteuttaa sekä koko organisaation että yksittäisten järjestelmien ja toimintatapojen tasoilla, jotta voidaan varmistaa, ettei henkilötietoja vuoda väärille tahoille. Viimeinen Plegerin ja muiden esittelemä näkökulma on tietosuojan subjektiivisuus. Yksilöiden kiinnostus omaan tietosuojaan on puutteellista, mutta paljastukset tietomurroista ja yritysten epäeettisistä toiminnoista tietosuojan osalta ovat kasvattaneet tietoisuutta väestössä. Subjektiiviseen kokemukseen tietosuojasta vaikuttaa muun muassa kulttuurinen tausta, henkilön luottavaisuus ja riskinottohalu.

2.3 Yleinen tietosuoja-asetus GDRP

Yleinen tietosuoja asetus eli General Data Protection Regulation (GDRP) on Euroopan Unionin asettama asetus, jolla turvataan henkilöiden tietojen asianmukaista käsittelyä. Täysimääräisesti asetusta on ruvettu soveltamaan Euroopan Unionin alueella keväästä 2018. Yleisellä tietosuoja-asetuksella pyritään edistämään henkilötietojen suojaa, yhdenmukaistamaan tietosuojalainsäädäntöä Euroopan unionissa, luomaan alueelle sisämarkkinoita, sekä vastaamaan globalisaatiosta ja digitalisaatiosta nousseisiin tietosuojakysymyksiin. Yleinen tietosuoja-asetus määrittelee huomattavan paljon vaatimuksia henkilötietoja käsitteleville organisaatioille. Tällaisia vaatimuksia ovat esimerkiksi vaatimukset rekisteröidyn tietojen korjaamisesta ja poistamisesta tämän niin pyytäessä. Henkilötietorekisterin pitäjän tulee pyynnöstä luovuttaa tälle kaikki rekisteröidyn tiedot. Tietojen luovuttamisen lisäksi rekisterinpitäjän täytyy perustella miksi ja miten hän henkilötietoja käsittelee. Asetus vaatii myös henkilötietojen käsittelylle perusteen. Perusteena voi olla muun muassa erillinen suostumus, sopimus, yleinen etu, lakisääteinen velvoite tai elintärkeän edun suojaaminen. Suurempien rekisteriä pitävien organisaatioiden (yli 250 työntekijää) on tehtävä julkinen seloste henkilötietojen käsittelystä. Myös alle kahdensadanviidenkymmenen työntekijän organisaatioilta vaaditaan samanlainen seloste, mikäli henkilötietojen käsittely ei ole satunnaista tai käsiteltävät henkilötiedot ovat arkaluontoisia. (tietosuoja.fi, 2022)

Tarve luoda uusi tietosuoja-asetus on seurausta nopeasta yhteiskunnan digitalisaatiosta ja teknologian kehityksestä. Yritysten liiketoiminnassa asiakkaiden henkilötiedoilla on aiempaa suurempi merkitys ja näitä myös käsitellään yrityksissä aiempaa enemmän. Tiedon onkin sanottu olevan uuden ajan öljy ja Euroopan unioni on lainsäädännöllä halunnut turvata tätä arvokasta tietoa. Euroopassa tietosuoja on koettu jo kauan ihmisoikeutena ja jo ennen GDPR:n säätämistä, Euroopan Unionin alueella oli voimassa vuonna 1995 voimaan tullut tietosuojadirektiivi. Direktiivillä pyrittiin yhtenäistämään EU-alueen

tietosuojalainsäädäntöä, sillä erilaisten lakien pelättiin heikentävän alueen sisämarkkinoita. Direktiivi ei onnistunut tarkoituksessaan ja sitä jouduttiin paikkaamaan kansallisilla laeilla. Direktiivin rikkomisesta ei voitu antaa tuntuvia sakkoja sen rikkojille ja esimerkiksi vuonna 2007, Ranska antoi Facebookille tietosuojarikkeistä vain 150 000 euron sakon. Direktiivillä ei siis ollut riittävää pelotevaikutusta, jotta yritykset panostaisivat tietosuojaan tarvittavalla vakavuudella. Näitä ja muitakin puutteita ratkoakseen Euroopan Unioni aloitti uuden tietosuojalainsäädännön valmistelun vuonna 2009. (Hoofnagle, Sloot & Borgesius, 2019).

Tietosuojavaltuutetun toimiston mukaan yleisen tietosuoja-asetuksen tarkoituksena on ollut: ”parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa sekä edistää digitaalisten sisämarkkinoiden kehittymistä.”. Laki määrittelee yksilölle seuraavia oikeuksia:

- tietää mitä henkilötietoja organisaatiolla on sinusta
- tietää miten ja mihin tarkoitukseen henkilötietojasi käsitellään
- pyytää virheellisten, epätarkkojen ja puutteellisten henkilötietojesi korjaamista
- pyytää henkilötietojesi poistamista
- vastustaa henkilötietojesi käsittelyä
- pyytää henkilötietojesi käsittelyn rajoittamista
- siirtää tietosi toiselle organisaatiolle
- olla joutumatta perusteetta automaattisen päätöksenteon kohteeksi.

Yleisessä tietosuoja-asetuksessa määritellään periaatteet, joiden mukaan henkilötietoja voidaan käsitellä. Näiden periaatteiden mukaan henkilötietoja on käsiteltävä lain- ja asianmukaisesti. Tietoja on kerättävä tiettyyn, tarkkarajaiseen ja lailliseen tarkoitukseen. Tietoja saa kerätä vain tarkoitusta varten tarpeellisen määrän, tietoja ei saa kerätä varmuuden vuoksi. Virheelliset tai puutteelliset tiedot tulee korjata. Tietoja saa säilyttää vain niin kauan, kun se on alkuperäisen keräysperusteen kannalta perusteltua. Tietoja on aina käsiteltävä luottamuksellisesti ja turvallisesti. Tarvittaessa rekisterin pitäjän tulee henkilötietoja käsitellessä pystyä esittämään, että tietosuojaperiaatteet toteutuvat aidosti. (tietosuoja.fi, 2022). Yleisessä tietosuoja-asetuksessa sen tavoitteeksi määritellään seuraavat asiat: vahvistetaan säännöt luonnollisten henkilöiden henkilötietojen käsittelylle, suojaamaan henkilöiden perusoikeuksia, etenkin tietosuojan osalta sekä varmistaa datan vapaa liikkuvuus unionin alueella. Viimeisellä halutaan varmistaa, että rekisterin pitäjä ei voi estää datan siirtopyyntöjä rekisteröidyn toimesta. (Yleinen tietosuoja-asetus, 2016/679,)

GDPR pyrkii parantamaan kansalaisten henkilötietojen suojaa kuuden ydinperiaatteen avulla. Nämä periaatteet ovat: oikeudenmukaisuus ja laillisuus, käyttöoikeuksien rajoittaminen, tietojen minimointi, tarkkuus, tiedon varastoinnin rajoitukset, sekä eheys ja luottamuksellisuus. Näitä ydinperiaatteita pyritään toteuttamaan lisäämällä läpinäkyvyys- ja tilivelvollisuusvaatimuksia yrityksille. Perustavanlaatuinen muutos aiempaan tietosuojalainsäädäntöön onkin vaatimus käyttäjän suostumukselle ja se tulee olla tarkasti rajattu tiettyyn tarkoitukseen. Lisäksi henkilötietorekisterin pitäjän täytyy saattaa suostumuksen

antamiseksi vaadittava tieto käyttäjälle ennen hyväksyntää. Perusteet tietojen käsittelylle täytyy olla asiakkaalle helposti ja saavutettavasti näkyvillä, esimerkiksi tietosuojaselosteen muodossa. Tilivelvollisuus taas vaatii henkilötietoja omaavan kantavan vastuun käsiteltävistä tiedoista ja niiden asianmukaisesta käsittelystä. Perustavanlaatuinen muutos aiempaan tietosuojalainsäädäntöön onkin vaatimus käyttäjän suostumukselle ja se tulee olla tarkasti rajattu tiettyyn tarkoitukseen. Lisäksi henkilötietorekisterin pitäjän täytyy saattaa suostumuksen antamiseksi vaadittava tieto käyttäjälle ennen hyväksyntää. (Goddard, 2017)

Suomessa kansallisella tasolla tietosuojaa käsittelee tietosuojalaki 5.12.2018/1050. Suomen kansallisen tietosuojalainsäädännön tehtävänä on täsmentää ja tarkentaa Euroopan Unionin tietosuoja-asetusta. Laissa määritellään useita erilaisia tilanteita ja käyttötapauksia, joissa yleisen tietosuoja-asetuksen kohtia tulkitaan. Laissa määritellään ikärajaksi 13 vuotta, jonka jälkeen tietoyhteiskunnan palveluita voidaan tarjota suoraan kansalaiselle, eikä tämän vanhemman kautta. Kansallisessa lainsäädännössä määritellään henkilötietojen käsittelylle erityistilanteita journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun perusteella. Suomessa tietosuojasta vastaava kansallinen valvontaviranomainen on tietosuojavaltuutettu. Tietosuojavaltuutetulla on apunaan toimisto, johon nimitetään ainakin kaksi apulaistietosuojavaltuutettua sekä muita alaan perehtyneitä asiantuntijoita. Tietosuojavaltuutettu ja apulaistietosuojavaltuutetut nimitetään viiden vuoden määräajoiksi valtioneuvoston toimesta.
(Tietosuojalaki, 1050/2018). Mazurin, Palinskyn ja Sobolewskin mukaan on kuitenkin hyvin mahdollista, että juuri kansallinen lainsäädäntö EU-maissa heikentää GDPR:n yhtä tarkoitusta digitaalisen sisämarkkinan luomisesta, sillä asetus sallii jonkin verran datankäsittelyyn poikkeuksia ja vapautta kansallisen lainsäädännön osalta.

3 GDPR:n vaikutukset yritysten toimintaan

Yleisen tietosuoja-asetuksen muuttaessa alan lainsäädäntöä suuresti, on sillä ollut myös suuria vaikutuksia yritysten toimintaan monella alalla. Tässä luvussa esitellään, mitä vaikutuksia GDPR on ensimmäisinä voimassaolovuosinaan aiheuttanut yrityksille. Vaikutuksia tutkitaan organisaatioiden henkilötietojen hallintaan, tietojärjestelmiin ja kustannuksiin.

3.1 GDPR:n vaikutukset yritysten datan hallintaan

GDPR:n vaatimusten täyttäminen on vaatinut yrityksiltä huomattavan määrän muutoksia tietojen käsittelemiseen. GDPR vaatii, että käyttäjän tietojen käsittely minimoidaan. Organisaatioiden täytyy pohtia aiempaa tarkemmin, mitkä tiedot ovat liiketoiminnan kannalta välttämättömiä, ja olla käsittelemättä muita tietoja. Yrityksiltä vaaditaan myös suunnitelmia siitä, kuinka tietoja aiotaan käsitellä. Mikäli tietoja siirretään toiseen maahan, on rekisterinpitäjän varmistettava, että kohdemaassa noudatetaan sekä GDPR:n, että kohdemaan lainsäädäntöä. Mikäli tietoja käsittelee alihankkija, tulee toimeksiantajaorganisaation varmistua siitä, että tietoja käsitellään oikein myös alihankkijan toimesta. Toiminta ja järjestelmät tulee rakentaa alusta alkaen GDPR -yhteensopiviksi. Tämä täytyy toteuttaa kaikilla toiminnan tasoilla. Esimerkiksi järjestelmää luodessa, tulee varmistaa, että järjestelmässä ei ole mekanismeja, joilla se keräisi ylimääräistä tietoa. Hankalaa on se, että asetus ei anna ohjeita tarpeeksi hyvistä ratkaisuista, vaan se jää yritysten oman harkinnan varaan. (Tikkinen-Piria, Rohunena, Markkula, 2017)

Asetus kannustaa organisaatiota luomaan Code of Conducteja eli eettisiä toimintaohjeita erilaisia tilanteita varten. Näillä toimintaohjeilla voidaan osoittaa organisaation sitoutumista asetuksen vaatimuksiin. Vapaaehtoisten tietosuojasertifikaattien hankinta on myös suositeltua. Tietosuoja-asetus vaatii rekisterinpitäjää ilmoittamaan viipymättä kaikista tietomurroista. Tämän aikaansaamiseksi organisaatioiden täytyy suunnitella ja valmistella aiempaa tarkemmin selkeät prosessit poikkeustilanteita varten. Asianomaisten tavoittaminen tehokkaasti voi olla hankalaa, joten kontaktointiprosessi tulee olla valmiiksi suunniteltu. Yleinen tietosuoja-asetus mahdollistaa huomattavien sanktioiden langettamisen yrityksille, jotka laiminlyövät asetuksen vaatimukset, joten todennäköisesti kaikki tiedonkäsittelyn prosessit tulee arvioida uudelleen tai vähintään tarkastaa. Asetus vaatii yrityksiä, jotka käsittelevät säännöllisesti henkilötietoja nimeämään tietosuojavastaavan (Data Protection Officer). Tämä voi olla hankalaa, sillä osaavia henkilöitä ei välttämättä löydy yrityksen sisältä. (Tikkinen-Piria, Rohunena, Markkula, 2017)

Yleisen tietosuoja-asetuksen mukana käyttäjille pitää informoida selkeästi, kuinka tietoja käytetään, joten yritysten tulee luoda tietosuojaselosteet käyttäjiensä näkyville. Asetuksen aiempaa tarkemmat suostumusvaatimukset aiheuttavat muutoksia yrityksissä. Yrityksillä täytyy siis olla lomakkeet tai muut tavat kysyä käyttäjän suostumus jokaisen tiedon käsittelyyn. Muun muassa, mikäli verkkosivusto käyttää mainonnan kohdentamiseen tai muuhun tarkoitukseen evästeitä, tulee tästä ilmoittaa ja pyytää käyttäjän lupa ennen kuin sivustoa voi käyttää. Rekisterinpitäjän tulee myös varmistua käyttäjän iästä (alle 13-vuotias ei voi antaa suostumusta) ja valvoa tätä. Käyttäjällä on oikeus tulla unohdetuksi, joten organisaatioiden tulee kehittää prosessit, joilla pyynnöstä voidaan poistaa kaikki tiedot käyttäjästä. Unohdetuksi tulemisen lisäksi käyttäjä voi vaatia tietoja itselleen tai siirrettäväksi toiseen järjestelmään. Tietojen siirtäminen voi olla erityisen haastavaa standardien puutteen takia. Kaikista näistä toimista tulee myös pitää ajantasaista dokumentaatiota. Rekisterinpitäjien tulee laatia ja ylläpitää kahta eri dokumenttia: selostetta käsittelytoimista, sekä tietosuojaa koskevaa vaikutusarviointia. Ensin mainittu kuvaa miten ja kuka henkilötietoja käsittelee. Toinen taas täytyy olla, jos käsitellään riskialttiita tietoja ja siinä tulee olla kuvaukset mahdollisista riskeistä ja toimintamalleista riskin realisoituessa. Molempien dokumenttien tulee olla nähtävissä valvovalle viranomaiselle. (Tikkinen-Piria, Rohunena, Markkula, 2017)

Koska GDPR:n mukaan pitää olla tiedossa, kuka tietoja käsittelee ja millä perusteella, olisi hyvä, että organisaatioiden käsittelemä tieto löytyisi kootusti yhdeltä serveriltä, johon pääsee kirjautumaan vain auktorisoidut henkilöt. Riskit väärinkäytöksistä kasvavat, kun tietoja löytyy useilta koneilta, joiden valvominen on haastavampaa. Tietoja käsiteltäessä tulee pitää huolta myös normaaleista tietoturvaan liittyvistä toimista, kuten salasanoista, välttämällä kalasteluviestejä, päivittämällä ohjelmistot ajantasaisiksi ja käyttämällä VPN:ää muussa kuin yrityksen verkossa toimiessa. Yrityksille voi olla hyödyllistä hankkia ulkopuolista apua auditoivilta yrityksiltä, jotta asetuksen vaatimukset saataisiin parhaiten täytettyä. (Tiliuțe, 2019)

GDPR:n teknologianeutraalius saattaa aiheuttaa ongelmia toimijoille toteuttaa asetuksen vaatimukset sovelluksissa ja järjestelmissä. Erityisesti haasteita kohtaavat pienemmät yritykset, joilla ei ole omaa kattavaa lakiosaamista yrityksessä eikä välttämättä resursseja niiden hankintaan. Yleinen tietosuoja-asetus ei myöskään aseta sovelluskehitykseen suoria vaatimuksia, joten vastuun jakautuminen tietosuojan toteutumisesta ei ole aivan selvää. Asetuksen voidaan arvella tulevaisuudessa vaikuttavan myös kolmansille osapuolille myytävien tietojen keräämiseen, kuten nettisivujen evästeisiin. Seurantaevästeiden suhteen on ollut epäilyä, ettei GDPR olisi auttanut asiaa juurikaan. Nykyään käyttäjälle täytyy evästeiden keräämiseen pyytää lupa ja kertoa kerätyille tiedoille käyttötarkoitus. Käyttäjät eivät kuitenkaan perehdy näihin selosteisiin, vaan useimmiten painavat hyväksyntäpainiketta suuremmin asiaa pohtimatta. Yleinen tietosuoja-asetus saattaa kuitenkin vähentää käyttäjistä kerättävän datan määrää, sillä perusteet tietojen keräämiselle ovat tiukentuneet ja rangaistukset rikkomuksista ovat kiristyneet huomattavasti. Tästä ei kuitenkaan ole saatu

empiiristä aineistoa. Järjestelmäkehityksen kannalta olisi mahdollisesti hyvä saada tarkentavaa ohjeistusta, jotta vastuut kehittäjien ja lopullisen rekisterinpitäjän välillä olisivat selkeämmät. Seurantatietoja käyttävien yritysten markkina on GDPR:n voimaantulon jälkeen keskittynyt harvemmille yrityksille. Alphabetin kaltaiset suuret yritykset ovat vallanneet alaa pienemmiltä entisestään, sillä liiketoimintaprosessien muokkaamiseen GDPR:n vaatimusten mukaisiksi on ollut enemmän lainopillisia resursseja. (Kollnig, Binns, Van Kleek, Lyngs & Zhao, 2021)

Yritysten näkökulmasta GDPR pyrkii yksinkertaistamaan yritysten ja henkilötietojen käsittelystä vastuussa olevien henkilöiden hallinnollista taakkaa. Aiemmin vaadittu ilmoitus valvontaviranomaiselle henkilötietojen käsittelystä poistuu, mutta säännöksiin sisällytetään velvoitteita ja periaatteita, jotka liittyvät suoraan yritysten hallintoon, riskienhallintamalleihin ja sääntöjen noudattamiseen. Uusiin henkilötietojen suojaa koskeviin periaatteisiin sisältyy muun muassa avoimuus tietojen käsittelytavassa, proaktiivinen vastuu periaatteiden noudattamisessa (tilivelvollisuus) sekä tietojen suojelu suunnittelusta alkaen (tietosuoja suunnittelussa) ja oletuksena tapahtuva tietojen suojaus. GDPR velvoittaa myös nimittämään tietosuojavastaavan suurimuotoista henkilötietojen käsittelyä harjoittaville yrityksille ja edistämään tietojen eettistä käsittelyä, sekä sertifiointimekanismien käyttöä. (Martínez-Martínez, 2018)

Yrityksille on luotu erilaisia työkaluja, joiden tarkoituksena on helpottaa vastaamista asetuksen vaatimuksiin ja datanhallinnan prosessien muuttamista lain vaatimukset täyttäviksi. Eräs tällainen työkalu kehitettiin osana Tietosuojavaltuutetun toimiston ja TIEKE Tietoyhteiskunnan kehittämiskeskus ry:n GDPR2DSM-hanketta. Hankkeen tarkoituksena oli parantaa mikro- ja pk-yritysten mahdollisuuksia asetuksen vaatimusten mukaiseen tietojenkäsittelyyn. Hankkeessa kehitetyn työkalun lähdekoodi on avoin ja näin kaikkien saatavilla. Työkalun lisäksi kerättiin muuta materiaalipankkia yritysten tueksi. Projekti toteutettiin EU-rahoituksen avulla vuosina 2020–2022. Ensimmäinen versio tietosuojatyökalusta julkaistiin kansainvälisenä tietosuojapäivänä 28.1.2022. Projektista kerätyn palautteen perusteella tietosuojatyökalu koettiin hyödylliseksi yrittäjän omalle perehtymiselle tietosuojaan. Lisäksi työkalun koettiin olevan hyvä apuväline organisaation henkilöstön kouluttamisessa. (TIEKE Tietoyhteiskunnan kehittämiskeskus ry, 2022)

Vuoden 2020 toukokuussa kaikki yritykset eivät vielä olleet toiminnassaan täysin GDPR-yhteensopivia. Zaeem ja Barber esittävät, että suurimpaan osaan GDPR:n vaatimuksista voidaan vastata jopa melko vaatimattomilla muutoksilla tietosuojapolitiikkaan, mutta ei kaikkiin. Osa vaatimuksista aiheuttaa organisaatioille suuren työmäärän. Tutkimuksessa analysoiduista yrityksistä 90 % oli jo saanut organisaationsa toiminnot päivitettyä vastaamaan asetuksen vaatimuksia. Tutkituilla organisaatioilla oli kuitenkin puutteita joidenkin vaatimusten osalta. Osa organisaatioista ei kerro tietosuojaselosteessaan, miten tai milloin tietomurroista ilmoitetaan viranomaisille eikä kerrota onko varastoitu data kryptattu vai ei. Joissakin tapauksissa ei vaadittu erillistä suostumusta käyttäjältä, joka asetuksen mukaan vaadittaisiin. Suurin osa verkkosivuista oli muuttanut jo

seurantaevästekäytäntönsä vastaamaan lakia. Tämä ei ole yllättävää, sillä rangaistukset rikkomuksista voivat olla mittavia. Puutteista huolimatta GDPR:n katsottiin vievän kuluttajan oikeuksia eteenpäin ja yritykset olivat huomioineet asetuksen hyvin. (Zaeem, Barber, 2020)

GDRP vaatii yrityksiä muuttamaan tietojenkäsittelyprosessejaan reilumpaan ja avoimempaan suuntaan. Prosessin täytyy läpinäkyvyyden lisäksi olla selkeä ja tarvittaessa dynaaminen. Perusteet tietojenkäsittelylle tulee myös esittää selkeällä kielellä, jotta kuluttaja oikeasti ymmärtää millä perusteilla tietoja käsitellään ja mihin niitä voidaan käyttää. Tietojenkäsittelyyn liittyviä prosesseja suunnitellessa suunnitelmat tulee rankentaa käyttäjäkeskeisiksi, jotta varmistutaan lainmukaisuudesta. (Goddard, 2017).

Asetuksen mukaan, jotta tietoja voidaan kerätä, täytyy sen olla tarpeellista liiketoiminnan tavoitteiden kannalta. Mikäli dataa ei enää tarvita, täytyy se poistaa. Ei välttämättä ole aina selvää, tarvitaanko jotain kerättyä tietoa vielä, vai onko siitä saatu hyöty jo maksimoitu. Organisaatioiden olisi hyvä kuvata tiedonkäsittelyprosessinsa tarkasti erilaisilla prosessikuvauksilla, jotta varmistutaan siitä, ettei turhia tietoja tallenneta. Yritykset voivat hyötyä myös auditointipalveluista varmistuakseen prosessien lainmukaisuudesta. (Basin, Debois, Hildebrandt, 2018)

Kirjassaan Voigt ja von dem Bussche esittelevät neliportaisen mallin, jonka mukaisesti voidaan muuttaa datan hallinnan prosesseja vastaamaan asetuksen vaatimuksia. Ensimmäisessä vaiheessa nykyiset prosessit täytyy analysoida eli suorittaa ns. GAP-analyysi. Vaiheen tarkoitus on saada kuva yrityksen prosessien nykytilasta ja analysoida mitä muutoksia tarvitaan, jotta prosessit saadaan halutunlaisiksi. Toisessa vaiheessa selvitetään kerättyyn dataan kohdistuvat riskit. Selvitetään asiat, jotka voivat negatiivisesti vaikuttaa rekisteröidyn henkilön oikeuksien toteutumiseen ja pyritään minimoimaan ne. Tässä vaiheessa olisi hyvä luoda tietosuojakonseptin alustava versio. Tietosuojakonsepti kuvaa perusperiaatteet tietojen suojatoimista ja vastuista. Kolmanneksi täytyy muutoksille varata tarvittavat resurssit ja määrätä projektin implementointi oikealle osastolle, kuten IT- tai lakiosastolle. Viimeisessä vaiheessa muutokset viedään tuotantoon ja henkilöstö koulutetaan tarvittaessa toimimaan lain vaatimalla tavalla, kun henkilötietoja käsitellään. (Voigt, von dem Bussche, 2017)

Asetuksen vaatimuksiin vastaaminen ei ole aina helppoa. Asetus itsessään on monimutkainen, monialalainen sekä se vaatii paikoin subjektiivista tulkintaa. Yhteensopivuuden saavuttaminen vaatii aikaa ja huomattavan määrän resursseja sekä henkilöstön työajan että kustannusten muodossa. Puutteellinen osaaminen sekä vähäiset käytännön oppaat vaikeuttavat työtä entisestään. Onnistuneen muutoksen mahdollistajina pidetään hyvää suunnitelman tiekarttaa, riskien tunnistamista, dokumentointia, henkilöstön laadukasta koulutusta sekä sopivien tietosuojavastaavien valitsemista. Onnistuneilla toimilla saavutetaan parempi läpinäkyvyys, mahdollisuuksia hyvään data-analytiikkaan ja kohonneeseen maineeseen kuluttajien silmissä. (Teixeira, da Silva, & Pereira, 2019). Axinten, Petrican ja Bacivarovin mukaan muutokset ovat selvästi niin suuria, että se muuttaa yritysten strategioita Eurooppaa koskien.

Cormackin mukaan asetuksella on usein negatiivinen konnotaatio lakina, joka mahdollistaa suurten sakkojen antamisen yrityksille, mutta se voidaan nähdä myös oppaana ja ohjeistuksena parempaan järjestelmäkehitykseen. Asetuksella ja sen implementoinnilla voi olla myös positiivisia vaikutuksia yritysten maineelle. Kansalaisilla on usein epäileviä tunteita suuria datamääriä hallinnoivia globaaleja suuryrityksiä kohtaan. Uuden, tiukemman lainsäädännön myötä kansalaisten luottamus dataa käsitteleviin yrityksiin ja näiden toimintaan voi nousta. (Cormack, 2021)

3.2 GDPR:n kustannusvaikutukset yrityksille

Tutkiessa yleisen tietosuoja-asetuksen vaikutuksia yritysten tuottomarginaaleihin huomattiin, että vuosina 2014-2018, kun yrityksissä valmistauduttiin GDPR:n voimaantuloon ei muutosta ollut juuri havaittavissa. Tulokseen vaikutti teollisuusalan yritysten osuus tutkimuksessa. Teollisuuden alalla asiakkaiden henkilötietojen merkitys on melko pientä, joten on oletettavaa, ettei henkilötietolainsäädännön muutoksilla olisi merkittävää vaikutusta. Vaikka yleisellä tasolla tarkasteltuna GDPR:n voimaantulo ei merkittävästi vaikuttanut yritysten kannattavuuteen, henkilötietoja vahvasti hyödyntävillä aloilla toimivien yritysten kohdalla tilanne oli toinen. Kun verrattiin eurooppalaisia ja yhdysvaltalaisia yrityksiä, joiden liiketoiminnassa asiakkaiden henkilötiedoilla oli merkittävä osa, huomattiin eurooppalaisten yritysten tuotto-osuuden kasvaneen 1,4–3,4 prosenttiyksikköä vähemmän kuin yhdysvaltalaisten kilpailijoiden. Suhteellisesti eniten voittomarginaalien laskua tapahtui eurooppalaisissa yhtiöissä, jotka ovat kooltaan pieniä tai keskisuuria. Verratessa eurooppalaisia ja yhdysvaltalaisia suuryrityksiä erot voittomarginaalien kehityksessä olivat huomattavasti pienempiä, jopa merkityksettömiä. Tutkimuksessa arvioitiin, että vaikka GDPR:n takia tehdyt investoinnit heikensivät eurooppalaisten yritysten kannattavuutta hetkellisesti, investoinnit saattavat luoda kilpailuetua pitkässä juoksussa. (Koski & Valmari, 2020)

On esitetty GDPR:n noudattamisen mahdollisesti haittaavan pk-yritysten kehitystä ja kilpailukykyä, sillä sen vaatimuksien noudattaminen vie yrityksen käytössä olevia resursseja. Suuremmissa yrityksissä on usein enemmän resursseja allokoida myös asetuksen täytäntöönpanoon ja implementointiin. Erityisesti on tutkittu aloja, joilla pilviteknologialla on ollut rooli pk-yritysten pyrkiessä saamaan kilpailuetua globaaleihin suuryrityksiin verraten. (Wilkinson, 2018.)

Chen, Frey ja Presidente kertovat samankaltaisista tuloksista siitä keille GDPR:n vaikutukset ovat tulleet kalliiksi. Suurille yrityksille GDPR:n noudattamiseen liittyvät kulut ovat olleet huomattavasti pieniä yrityksiä helpommin hoidettavissa. Yleisen tietosuoja-asetuksen katsotaan myös laskeneen

verkkokauppojen myyntiä. Tutkimuksessa seuratuissa yrityksissä myynti oli laskenut asetuksen käyttöönoton jälkeen 2 % aiemmasta. Osa asiakkaista jättää verkossa ostoksensa tekemättä, koska eivät anna verkkokaupalle lupaa käsitellä tietojaan tietosuojaselosteen mukaisesti. Kaikkinensa Euroopan alueella toimivien yritysten kannattavuus laski keskimäärin 8 % tutkitussa joukossa asetuksen takia. Teknologiayritysten voitot olivat laskeneet 4 % keskimääräistä enemmän, vaikka liikevaihdon lasku oli lähellä keskiarvoa. Tämän epäsuhdan liikevaihdon ja voittojen laskun välillä katsotaan johtuvan markkinaosuuksien siirtymisestä pienyrityksiltä teknologiajäteille. (Chen, Frey & Presidente, 2022) Myös Jia, Zhe Jin ja Wagman raportoivat kustannusten nousua ja kilpailukyvyn heikkenemistä välittömästi asetuksen voimaan tulon yhteydessä, erityisesti teknologiasektorin yritysten kohdalla.

Implementaatiokustannusten ja kilpailutilanteen muutosten lisäksi GDPR on vaikuttanut yrityksiin myös rangaistusten kautta. Yleisen tietosuoja-asetuksen rikkomisesta voidaan tuomita sakkoihin, jotka ovat suuruudeltaan korkeintaan 4 % vuoden liikevaihdosta. Vaikka uusi tietosuoja-asetus antaa viranomaisille valtuudet antaa huomattavasti aiempaa tiukempia rangaistuksia rikkeistä, ei niitä ole pääosin annettu. Tietosuoja-asetuksen voimaantulon jälkeen viranomaiset antoivat pääosin melko matalia sakkoja, ja osa Euroopan unionin maista ei ollut toukokuuhun 2020 mennessä antanut ainoitakaan sakkoja GDPR-rikkomuksista. Sanktiot yleisen tietosuojan rikkomisesta sen alkuvaiheessa muistuttivat suuruudeltaan edeltävän lainsäädännön rangaistuksia (Wolff & Atallah, 2021)

Ruohosen ja Hjelppen tutkimuksen mukaan laiminlyönneistä langetetut sakkorangaistukset ovat olleet melko pieniä vaihdellen pääosin neljän ja 163 tuhannen välillä. Tutkimustuloksilla oli kuitenkin pitkä häntä, jolloin myös pieniä määriä suuriakin sakkoja oli annettu. Vaikka asetuksen voimaantulon jälkeen rangaistukset ovat olleet pääosin maltillisia, on myös suurempia rangaistuksia nähty ja voidaan ajatella rangaistuskäytännön muuttuneen, kun Ranskan viranomaiset sakottivat googlea 50 miljoonalla eurolla. Suurempien sakkojen lisäksi niitä annettiin vuosina 2019–2020 huomattavasti enemmän kuin vuonna 2018. (Presthus & Sønslien, 2021). Toistaiseksi suurin GDPR:n mukainen langetettu sakko on 1,2 miljardia. Tämän sakon langetti Irlannin tietosuojaviranomainen (Irish Data Protection Authority (IE DPA)) Facebookin omistavan Metan Irlannin osastolle Meta Platforms Ireland Limitedille huhtikuussa 2023. Yritys ei ollut muuttanut lainvastaisia datanhallintaprosessejaan kuudessa kuukaudessa viranomaisen huomautuksesta huolimatta (European Data Protection Board, 2023). Voi siis olla, että tulevaisuudessa sakkojen vaikutus yritysten kustannuksiin kasvaa, jos sakot määrätään rangaistusasteikon yläpäästä.

Laybatsin jan Daviesin mukaan suurin osa yrityksistä on suunnitellut ja toteuttanut asetuksen vaatimat muutokset melko lailla suosiolla. Nousevat kustannukset ja lisätyö prosessihallintaan on aiheuttanut myös vastareaktioita. Esimerkiksi Facebookin omistava yritys on ollut välillä kriittinen lain vaateita kohtaa. Yritys aikoo noudattaa asetuksen vaateita Euroopassa, mutta aikoo siirtää muualla asuvien käyttäjiensä tiedot pois Euroopassa sijaitsevista datakeskuksistaan. Tällä yritys pyrkii minimoimaan asetuksen vaikutuksen

liiketoimintamalliinsa ja kannattavuuteensa. Muitakin kriisisesti asetukseen suhtautuvia teknologiayrityksiä löytyy etenkin Yhdysvalloista. Artikkelissaan Greengard kertoo myös osan yrityksistä olevan huolissaan GDPR:n vaikutuksista innovointiin. Asetus voisi heikentää mahdollisuuksia innovointiin esimerkiksi robotiikan, autonomisten ajoneuvojen ja muihin tekoälypohjaisiin sovelluksiin. Pitkässä juoksussa heikentyvät innovaatiomahdollisuudet voivat heijastua myös kilpailukykyyn.

Vaikka yleinen tietosuoja-asetus vaikuttaa eniten eurooppalaisiin yrityksiin, on sillä vaikutusta myös aasialaisiin ja yhdysvaltalaisiin yrityksiin. Yritysten tulee käyttää resursseja ja työvoimaansa päivittääkseen teknologia-alustoja, yksityisyyskäytäntöjään, mainonnan toimintamalleja ja muuttaa tietovarastointia sekä datan hallinnan prosesseja. Globaalien suurvaltojen Yhdysvaltojen ja Kiinan yritykset joutuvat myös päivittämään toimintaansa, koska niillä on useimmiten toimintaa EU:n alueella. 68 % yhdysvaltalaisyrityksistä ennustaa käyttävänsä yhdestä kymmeneen miljoonaa dollaria täyttääkseen GDPR vaatimukset ja 9 % yrityksistä arvelee käyttävänsä yli kymmenen miljoonaa dollaria. Kustannusten nousu saattaa näkyä myös asiakkaille nousseina hintoina. Ne yritykset, jotka onnistuvat luomaan parhaat ja tehokkaimmat tietosuojaprosessit saattavat saada merkittävää kilpailuetua tulevaisuudessa. (Li, Yu & Wu, 2019).

Enrothin tekemän selvityksen mukaan noin neljännes (23 %) arvioi yleisen tietosuoja-asetuksen vaikuttavan toimintaansa hyvin paljon tai paljon. 26 % vastaajayrityksistä epäili, että vaikutukset toiminnalle ovat pieniä tai olemattomia. Vastaajista suuremmat yritykset arvioivat vaikutusten olevan toiminalleen suurempia kuin pienet yritykset. Osa vastanneista pienyrityksistä ei osannut lainkaan vastata kysymykseen yrityksen henkilötietojen käsittelystä. On mahdollista, että suuremmilla yrityksillä on paremmat mahdollisuudet arvioida asetuksen vaikutuksia toimintaansa verrattuna pieniin tai keskisuuriin yrityksiin. Suurimpina kustannuksia nostavana toimena pidettiin tietojärjestelmien muuttamista GDPR-yhteensopiviksi. (Enroth, 2017)

Yksittäisten yritysten lisäksi aseuksella on kokonaisiin vaikutusta kokonaisiin markkinoihin. Henkilötietojen käyttöön perustuva liiketoiminta on valtaisa toimiala, mutta mikäli suuri määrä käyttäjiä päättää olla antamatta suostumusta tietojensa käytölle supistaa se alan markkinoita. On mahdollista, että GDRP toimii lainsäädäntönä suunnannäyttäjänä esimerkiksi muillekin alueille maailmanlaajuisesti, jolloin GDPR:n alueellinen vaikutus ei korostu samalla tavalla. (Aridor, Che, Salz, 2020)

4 Yhteenveto

Euroopan Unionin tietosuoja-asetusta voidaan pitää merkittävimpänä digiajan lainsäädäntömuutoksena henkilötietojen käsittelyyn. Se on aiheuttanut yrityksille ja muille organisaatioille suuria muutosvaatimuksia. Vastatakseen näihin muutosvaatimuksiin organisaatioiden on täytynyt muuttaa prosessejaan sekä usein myös perustavanlaatuista suhtautumistaan asiakkaidensa dataan. Asetus on vaikuttanut ainakin jossain määrin käytännössä kaikkiin Euroopan unionin alueella toimiviin yrityksiin. Asetuksen vaikutukset eivät kuitenkaan ole olleet samanlaisia kaikille organisaatioille. Esimerkiksi organisaatioiden koot ja toimialat ovat määrittäneet sitä, kuinka helposti lain asettamiin vaatimuksiin on saatu vastattua.

Tässä tutkielmassa pyrittiin selvittämään Euroopan unionin yleisen tietosuoja-asetuksen vaikutuksia. Yleisen tietosuoja-asetuksen laajuuden takia tutkimuksen kohteet rajattiin muutamaan teemaan: vaikutus yritysten kannattavuuteen, asetuksen kustannusvaikutukset yrityksille sekä vaikutukset ja haasteet datahallintaprosesseihin, joissa käsitellään henkilötietoja.

- Millaisia vaikutuksia GDPR:llä on ollut yritysten datan hallintaan?
- Millaisia kustannusvaikutuksia GDPR:llä on ollut organisaatioille?

Tutkielman ulkopuolelle rajattiin esimerkiksi tarkemmat tekniset muutokset organisaatioiden tietojärjestelmiin.

GDPR:n vaatimuksiin vastaaminen on vaatinut yritysten datanhallintaan mittavia muutoksia. Nämä muutokset liittyvät tarkempaan henkilötietojen käsittelyn suunnitteluun, alihankkijoiden valvontaan, henkilötietojen käsittelyn minimointiin, GDPR-yhteensopivien järjestelmien rakentamiseen ja dokumentointiin. Asetus kannustaa lisäksi eettisten ohjeiden luomiseen ja sertifiointiin. Yritysten on ilmoitettava aiempaa tiukemmin tietomurroista ja kehitettävä prosesseja poikkeustilanteiden varalta. Yritysten tulee myös uuden lainsäädännön myötä noudattaa selkeämpiä suostumusvaatimuksia. Lisäksi tietojen säilyttämisen ehdot ovat tiukentuneet. Pienemmille yrityksille datan hallintaan liittyvät vaatimukset ovat olleet usein hankalia. Tämän takia markkinat ovat keskittyneet isommille toimijoille. Yritysten avuksi on kehitetty erilaisia työkaluja ja materiaalipankkeja, joiden avulla vastaaminen asetuksen vaatimuksiin olisi helpompaa. Esimerkiksi tietosuojavaltuutetun toimisto ja oikeusministeriö julkaisivat Miten valmistautua EU:n tietosuoja-asetukseen? -oppaan vuonna 2017. Oppaassa annetaan ohjeita rekisterinpitäjälle ja käydään asetuksen vaateita kohta kohdalta ja annetaan käytännön ohjeita ja esitellään asetuksen pääkonsepteja organisaatioiden näkökulmasta. (Tanus, Hänninen, Pihamaa, 2017)

Yleisellä tietosuoja-asetuksella on ollut useita vaikutuksia yritysten kilpailukykyyn ja kustannuksiin monella tavalla. Tutkimuskirjallisuuden mukaan GDPR:n voimaantulo ei ole merkittävästi vaikuttanut yritysten

kannattavuuteen. Vaikutuksissa kannattavuuteen esiintyi eroja toimialoittain, sekä yritysten koon mukaan. Verrattuna yhdysvaltalaisiin kilpailijoihin henkilötietoja vahvasti hyödyntävillä aloilla toimivien eurooppalaisten yritysten voittomarginaalit laskivat hieman. Tämä tapahtui selkeämmin pienten ja keskisuurten yritysten kohdalla. Suurten yritysten kohdalla tämän kaltaista vaikutusta ei merkittävissä määrin havaittu. Asetuksen aiheuttamat kustannukset muodostavat etenkin pienemmille yrityksille suhteellisesti mittavia haasteita. Tämä on pois näiden yritysten käytössä olevista resursseista, joilla olisi voitu pyrkiä parantamaan yritysten kilpailukykyä. Toisaalta investoinnit GDPR:n noudattamiseen ja yksityisyyttä kunnioittavampiin prosesseihin saattavat kuitenkin tuoda pitkällä aikavälillä kilpailuetua. Asetuksen myötä verkkokauppojen myynnissä on tapahtunut pientä laskua heti asetuksen käyttöönoton jälkeen.

GDPR:n rikkomisesta voidaan määrätä aikaisempaa huomattavasti suurempia sakkoja yrityksille. Pääosin annetut sakot ovat olleet melko pieniä, mutta myös huomattavia sakkoja on annettu räikeistä rikkomuksista. Sakkojen vaikutus saattaa kasvaa tulevaisuudessa, mikäli tavaksi vakiintuu sakkojen määrääminen rangaistusasteikon yläpään mukaan. Sakot määräytyvät yrityksen liikevaihdon mukaan, joten sakot tuntuvat huomattavilta myös suuremmissa yrityksissä.

Vaikka GDPR on aiheuttanut muutosvaatimuksia käytännössä kaikille yrityksille, jotka toimivat EU:n alueella, on yritysten ominaisuuksilla ollut vaikutusta siihen, kuinka helposti lain asettamiin vaatimuksiin on voitu vastata. Hankalimpia muutokset ovat olleet pienille ja keskisuurille yrityksille. Näissä yrityksissä ei usein ole valmiuksia välittömästi vastata tämän tason lainsäädäntömuutoksiin.

Koon lisäksi yritysten toimialoilla on huomattavaa vaikutusta siihen, kuinka suuria haasteita uusi yleinen tietosuoja-asetus on niille aiheuttanut. Kuten ennalta voitiin arvella, yrityksillä, joiden liiketoiminnalle henkilötietojen käsittelyllä oli pienempi rooli, oli myös sopeutuminen uuteen lainsäädäntöön helpompaa. Perinteisen raskaan teollisuuden yrityksille GDPR ei siis aiheuttanut toimintaan, kannattavuuteen tai kulurakenteeseen suurempia muutoksia. Korkean teknologian – ja etenkin asiakkaiden tiedoilla tuloksensa tekevät yritykset joutuivat muuttamaan toimintaa jo huomattavasti. Esimerkkejä jälkimmäisistä ovat sosiaalisen median suuryritykset, kuten Twitter, Facebookin ja Instagramin omistava Meta Platforms Inc. ka hakukonejätti Googlen omistava Alphabet Inc.

Euroopan unionin yleisessä tietosuoja-asetuksessa on tutkimusaihetta erilaisille tutkimussuunnille ja jo tätä tutkielmaa voisi jatkaa useisiin suuntiin. Tutkimuksen kannalta kiinnostavaa olisi selvittää, kuinka suomalaiset yritykset ovat vastanneet GDPR:n asettamiin haasteisiin, ja millaisia toimia ne ovat joutuneet toteuttamaan. Alueellisen tutkimuksen lisäksi lienee arvokasta tutkia eri toimialojen tietojärjestelmämuutoksia. Tässä tutkielmassakin on esitetty eri toimialojen olevan huomattavan erilaisessa asemassa vastatessaan uuden lainsäädännön asettamiin vaatimuksiin. Erityisesti tutkimusta voisi olla mielekästä kohdentaa henkilötietointensiivisten alojen yrityksiin. Tällaisia yrityksiä olisivat esimerkiksi sosiaaliseen mediaan keskittyneet yritykset kuten Meta Platforms Inc.

tai liikevaihtonsa asiakkaiden tiedoilla saavat yritykset, kuten Googlen omistava yritys Alphabet Inc. Näitä globaaleja yrityksiä tutkimalla saataisiin vertailtua myös siitä, kuinka asetus on vaikuttanut kannattavuuteen, kun voidaan verrata saman ajanjakson liiketoimintadataa alueilta, joissa GDPR on voimassa ja alueilta, joissa ei.

Tutkielman kirjoitushetkellä yleinen tietosuoja-asetus on ollut voimassa noin viisi vuotta. Tulevaisuudessa voidaankin tutkia, sitä millaiset vaikutukset asetuksella on pidemmällä aikavälillä tarkasteltuna. Tuoko uusi lainsäädäntö mahdollisesti liiketoiminnallista etua eurooppalaisille (tai Euroopassa toimiville) yrityksille, vai aiheuttaako se vain lisävaivaa ja -kustannuksia.

Lähteet

1.2 billion euro fine for Facebook as a result of EDPB binding decision. (22.5.2023). European Data Protection Board edpb.
https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Aridor, G., Che, Y.-K., & Salz, T. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR. NBER Working Paper Series.

Asetus 2016/679. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan parlamentti ja neuvosto. *https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679*

Axinte, S.-D., Petrică, G., & Bacivarov, I. (2018). GDPR Impact on Company Management and Processed Data. *Quality Access to Success, 19(165)*

Basin, D., Debois, S., & Hildebrandt, T. (2018). On Purpose and by Necessity: Compliance Under the GDPR. *Lecture Notes in Computer Science, 10957. https://doi.org/10.1007/978-3-030-03840-3*

Chen, C., Frey, C., Presidente, G. (2022) Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *The Oxford Martin Working Paper Series on Technological and Economic Change*

Cormack, A. (2021). Thinking with GDPR: A guide to better system design. Information Services & Use, 41, 61-69.

Enroth, T. O., & Neuvonen, R. J. P. (2017). EU:n tietosuoja-asetuksen yritysvaikutukset. Finland. Valtioneuvoston Kanslia. Julkaisusarja, Nro 10/2017, Valtioneuvoston kanslia, Helsinki.

Euroopan komission verkkosivut (20.7.2022) Data protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Goddard, M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research Vol. 59 Issue 6*

Greengard, S. (2018). Weighing the Impact of GDPR. *Communications of the ACM, 61(11), 16-18. doi:10.1145/3276744*

Jia, J., Jin, G. Z., & Wagman, L. (2019). The Short-Run Effects of GDPR on Technology Venture Investment.

Hoofnagle, C., van der Sloot, B. & Borgesius F. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law, 28:1, 65-98*

Kollnig, K. & Binns, R. & Van Kleek, M. & Lyngs, U. & Zhao, J. & Tinsman, C. & Shadbolt, N. (2021). Before and after GDPR: tracking in mobile apps. *Internet Policy Review, 10(4). https://doi.org/10.14763/2021.4.1611*

Koski, H., Valmari, N. (2020) Short-term Impacts of the GDPR on Firm Performance. *ETLA Working Papers, No. 77, The Research Institute of the Finnish Economy (ETLA), Helsinki*

Li, H., Yu, L., & Wu, H. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management, 22(1), 1-6. DOI: 10.1080/1097198X.2019.1569186.*

Laybats, C., & Davies, J. (2018). General Data Protection Regulation: Implementing the regulations. *Business Information Review, 35(2), 81-83. https://doi-org.libproxy.tuni.fi/10.1177/0266382118777808*

Martínez-Martínez, D.-F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *El profesional de la información, 27(1), 185-194. https://doi.org/10.3145/epi.2018.ene.17*

Mazur, J., Palinski, M., & Sobolewski, M. (2017). GDPR: A Step Towards a User-centric Internet? Intereconomics, 52(4), 207-213.

Pangrazio L., Selwyn N. (2018). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society. 2019;21(2):419-437. doi:10.1177/1461444818799523*

Petticrew, M (2001). Systematic Reviews from Astronomy to Zoology: Myths and Misconceptions. *British Medical Journal 322: 7278, 98–101.*

Pleger, L., Guirguis, K., Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior ,Volume 122, 2021, https://doi.org/10.1016/j.chb.2021.106830.*

Presthus, W., Sønslien, K., (2021) An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management: Vol. 9 : No. 1 , Article 3.*

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. *Information Systems, 106, 101876.*

Salminen, A (2011) Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppei-hin ja hallintotieteellisiin sovelluksiin, Vaasan Yliopisto

Talus, A., Autio, E., Hänninen, A., Pihamaa, H.-T., & Kantonen, S. (2017). Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu, 4/2017.

Teixeira, G., Mira da Silva, M. & Pereira, R. (2019). The critical success factors of GDPR implementation - a systematic literature review. *Digital Policy, Regulation and Governance. 21 (4), 402-418.*

Tietosuoja.fi (12.8.2022) *https://tietosuoja.fi/etusivu*

Tietosuojalaki, 1050/2018

TIEKE Tietoyhteiskunnan kehittämiskeskus ry. (31.01.2022). GDPR2DSM – Tietosuojaosaamista pk-yrityksille 2020-2022. https://tieke.fi/hankkeet/gdpr2dsm/

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34(1), 134-153.*

Tiliute, D. (2019). GDPR and its impact on IT departments of companies. *The USV Annals of Economics and Public Administration, 19(2), 30.*

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide.

Wolff, J., Atallah, N., (2021) Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020. *Journal of Information Policy 1 December 2021; 11 63–103. doi: https://doi.org/10.5325/jinfopoli.11.2021.0063*

Wilkinson, G. (2018). General data protection regulation: No silver bullet for small and medium-sized enterprises. Journal of Payments Strategy & Systems, 12 (2), 139-149.

Zaeem, R. N., Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems, 12(1), DOI: 10.1145/3389685.*