Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

NLIIBK14

2018

Peter Palmroth

PK-YRITYKSEN VALMISTAUTUMINEN EU:N TIETOSUOJA-ASETUKSEEN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous & Tietojenkäsittely

2018 | 20 sivua

Peter Palmroth

PK-YRITYKSEN VALMISTAUTUMINEN EU:N TIETOSUOJA-ASETUKSEEN

Tämä opinnäytetyö on osa laajempaa projektia toimeksiantajayritykselle, jonka tarkoituksena oli päivittää yrityksen tietoturva ja henkilötietojen käsittelyn prosessit tietosuoja-asetuksen 2016/679 mukaisiksi. Opinnäytetyössä tutkitaan tietosuoja-asetuksen voimaantulon johdosta syntyneitä toimenpiteitä ja muutoksia prosesseihin, dokumentointiin sekä tietoturvaan.

Teoriaosuudessa käydään läpi tietosuoja-asetuksen suurimpia muutoksia, toimeksiantajan käytössä olevia laitteita, ohjelmistoja ja järjestelmiä, niiden ominaisuuksia ja konfigurointia GDPR-määräysten mukaisiksi. Tutkimusmenetelmänä opinnäytetyössä käytettiin kvalitatiivista tutkimusta. Projektin toteutuksessa hyödynnettiin EU:n tietosuoja-asetusta, ulkomaista materiaalia sekä monia luentoja ja koulutuksia joista osa oli maksullisia.

Case-osiossa pureudutaan syvemmälle toimeksiantajan prosesseihin, niiden yhdenmukaistamiseen ja käytössä olevien järjestelmien konfigurointiin ja tietoturvaan. Toimeksiantajan tarpeesta tehtiin myös tarkka kartoitus henkilötietoja sisältävistä rekistereistä, niiden ajantasaisuudesta ja käsittelystä. Yhteistyökumppaneiden toiveesta myös sähköpostit muutettiin salatuksi ja sähköposteissa sekä pilvessä lähetettävää dataa ja sähköpostin liitetiedostoja alettiin myös valvoa, jotta henkilötietoja tai muuta arkaa dataa ei ole edes mahdollista lähettää toimialueen ulkopuolelle ilman pätevää syytä. Toimeksiantaja toimii myös osana valtakunnallista ICT-toimijoiden ketjua, josta tuli myös ketjutasolta lisävaatimuksena FINCSC (Finnish Cyber Security Certificate), jolla voidaan todistaa yrityksemme tietoturva ja -suoja kumppaneille sekä asiakkaille.

ASIASANAT:

GDPR, tietoturva, tietosuoja-asetus

BACHELOR´S / MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business & Information Technology

2018 | 19 pages , 1 attachments

Peter Palmroth

PREPARING FOR GDPR FROM SMALL AND MEDIUM SIZE BUSINESS POINT OF VIEW

This thesis is a part of a wider project for an employer, which's purpose was to update the company's data security and the processes of treating private personal data so that they meet the standards of the General Data Protection Regulation (GDPR) 2016/679. The thesis will examine the generated measures and changes in the established processes, documentation and data security that were caused by the GDPR. In the theoretical section the thesis will present the major changes GDPR brings with it, the hardware, software and systems used by the company as well as their qualities and configuration to meet the standards of GDPR. The used research method in the thesis was qualitative content analysis. EU's regulation, foreign material as well as several seminars and paid training sessions were used to implement the project.

In the case section the thesis will concentrate heavily on the company's processes, in their standardization and the configuration of systems in use and data security. A comprehensive survey of the registers containing personal data, the data being up-to-date, and the processes of treatment were executed due to the need of the company. Due to the wishes of affiliates all emails were encrypted and the data as well as attachments flowing through it and the cloud service were started to oversee. This was done to prevent personal data or other sensitive information could not be sent outside of the domain without an adequate explanation. The company works also as a part of a national ICT-operators' franchise, which also demanded a FINCSC (Finnish Cyber Security Certificate), which can be used to certify the company's standards in data security and protection for the partners and customers.

KEYWORDS:

GDPR, information security, General Data Protection Regulation

SISÄLTÖ

LIITTEET

Lyhenne	Lyhenteen selitys (Lähdeviite)
Anonymisointi	Anonymisointi tarkoittaa tiedon muuttamista siten, että kyseistä tietoa ei voi yhdistää henkilöön. Anonymisoitu tieto ei ole henkilötieto (Holopainen 2018, 6.).
Henkilötieto	Henkilötieto on luonnolliseen henkilöön yhdistettävissä olevaa tietoa (Holopainen 2018, 4.).
Henkilötietojen käsittelijä	Itsenäinen elinkeinon- tai toiminnanharjoittaja, joka käsittelee rekisterinpitäjän henkilötietoja (Holopainen 2018, 5.). Esimerkiksi alihankkija, joka hallitsee verkkokaupan ylläpitoa ja toimituksia.
Profilointi	Henkilötietojen automaattista käsittelyä, jossa henkilötietojen perusteella arvioidaan henkilön tiettyjä ominaisuuksia kuten terveys, kiinnostuksenkohteet ja sijainti (Holopainen 2018, 5.).
Pseudonymisointi	Käsitelty henkilötieto, jota ei voida yhdistää tiettyyn henkilöön ilman rekisteristä erillään olevia lisätietoja (Holopainen 2018, 6.).
Rekisteri	Henkilötietoja sisältävä jäsennelty tietojoukko, josta henkilötiedot ovat saatavilla tietyin perustein (Holopainen 2018, 5.).
Rekisterinpitäjä	Rekisterinpitäjä on rekisterin omistajayritys, jolla on myös oikeus määrätä rekisterin käytöstä (Holopainen 2018, 5.).
Rekisteröity	Henkilö, jonka henkilötietoja on rekisterissä (Holopainen 2018, 5.).
Suostumus	Vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilö ilmaisee esimerkiksi suostumuksensa hänen tietojensa käsittelyyn (2016/679 artikla 4).

1 JOHDANTO

Euroopan unionin parlamentti ja neuvosto antoi 27. huhtikuuta 2016 uuden asetuksen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Tietosuoja-asetus 2016/679.). Tietosuoja-asetus tunnetaan paremmin englanninkielisestä lyhenteestään GDPR (General Data Protection Regulation). Tietosuoja-asetus astui voimaan 25.5.2018.

Nopeasti kehittynyt teknologia vaatii uudenlaista säätelyä tietosuojasta huolehtimiseen. Tietosuoja-asetus luo selkeät peliohjeet ja kehykset yritysten henkilötietojen käsittelyyn, keräämiseen sekä luovuttamiseen. Kansalaisten näkökulmasta asetuksen tavoitteena on oman tiedon parempi hallinta. Tietosuoja-asetus suojaa erityisesti Euroopan unionin kansalaisia, joten kaikkien yritysten, kotipaikasta riippumatta, jotka toimivat Euroopan unionissa, pitää toimia samoilla säännöillä (Holopainen 2018, 3.). Tietosuoja-asetus ajaa yrityksen yhdenmukaistamaan ja dokumentoimaan prosessinsa, jotka koskevat henkilötietojen keräämistä, käsittelyä ja poistamista. Samalla myös vaaditaan riittävää tietosuojaa niin verkossa kuin kulunvalvonnan ja paperityöskentelyn osalta (Meling 2018).

Tiedon kerääminen, hallinta ja poistaminen tulee kansalaiselle läpinäkyvämmäksi ja helpommaksi kuin aiemmin. Rekisteröidyn laajentuneet oikeudet, kuten esimerkiksi saada häntä koskeva tieto yritykseltä itselleen ja jopa kokonaan tietojen poisto, eli oikeus tulla unohdetuksi, antaa kansalaiselle enemmän valtaa kasvavassa ja kehittyvässä tietoyhteiskunnassamme.

Aiheen valintaan vaikutti GDPR:n ajankohtaisuus ja toimeksiantoyrityksen toimeksianto asiaan liittyen. Tämän lisäksi toimin myös IT-alan yrityksessä konsulttina, joten toimeksiantoyrityksen asiakasyritykset ja aiheeseen liittyvän osaamisen käyttäminen liiketoiminnan kasvuun oli yhtenä syynä.

Tämän opinnäytetyön tavoitteena on havaita ja suorittaa uuden tietosuoja-asetuksen edellyttävät toimenpiteet ja vaikutukset asiakasyrityksessä. Varsinkin jo toimivien ympäristöjen, ohjelmistojen ja tilojen arviointi, dokumentointi ja muutostyöt ovat asioita joita jokainen pk-sektorin yritys joutuu miettimään saavuttaakseen riittävän tietoturvan tason tietosuoja-asetuksen mukaisesti. Tavoitteena on luoda organisaatiosta dokumentointi, jolla osoitusvelvollisuus täyttyy. Myös vaadittavat toimenpiteet riittävän tietosuojan varmistamiseksi ovat tärkeänä tavoitteena toimeksiantoyrityksen puolesta. Käytännössä

toimeksiantoyritys asetti tavoitteeksi opinnäytetyölle sen, että yrityksestä tulee laillinen rekisterinpitäjä. Opinnäytetyössä käytin tutkimusmuotona laadullista tutkimusta yhdistettynä laajaan empiirisen tutkimuksen kautta luotuun tietoon ja osaamiseen.

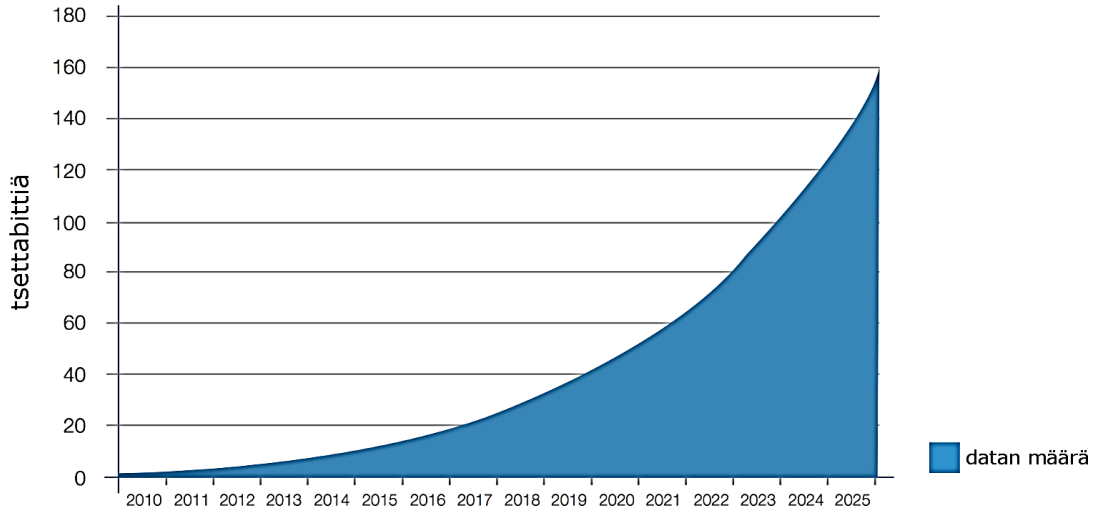
Toimeksiantaja opinnäytetyössä on perheyritys, jossa työskentelee noin 30 henkilöä. Alusta asti GDPR koettiin yrityksessä isoksi ja tärkeäksi muutokseksi, ja siihen piti löytää yrityksen sisältä vastuuhenkilö ajamaan asiaa eteenpäin.

2 EU:N TIETOSUOJA-ASETUS & MUUTOKSET

Euroopan unionin tietosuoja-asetus on iso uudistus alati kasvavaan tietoyhteiskuntaan, jossa elämme. Datan määrä on kovassa kasvussa ja tulee siitä vain kasvamaan. Tässä luvussa perehdytään Euroopan unionin tietosuojasäädöksen syihin, suurimpiin muutoksiin ja vaikutuksiin yleisellä tasolla. Samalla yritetään myös löytää ratkaisuja GDPR-yhteensopivuuteen yleisellä tasolla

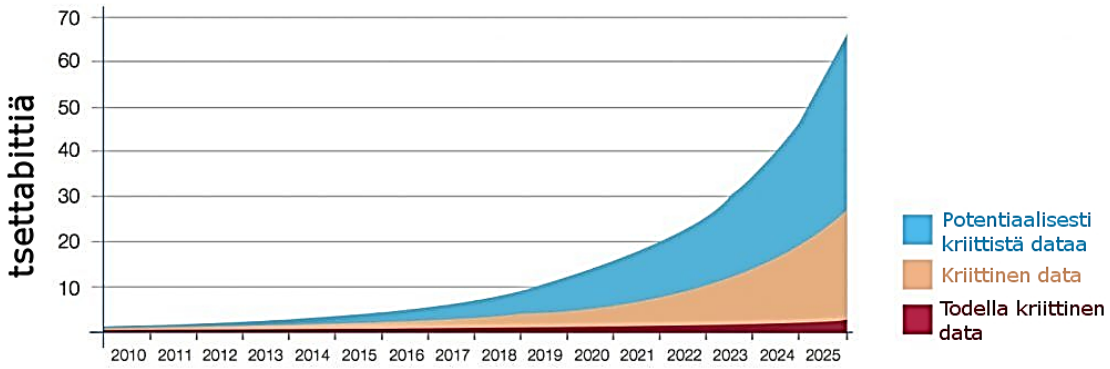
Datan määrän nopea kasvu

IDC:n Data Age 2025 tutkimuksessa oli selvinnyt, että ihmiskunnan alusta vuoteen 2003, oli digitaalista dataa luotu 5 miljardia gigabittiä dataa. Vuonna 2016 sama määrä dataa luotiin kahdessa päivässä. Esimerkiksi vuonna 2010 dataa oli noin 1 tsettabitti, ja ennusteiden mukaan vuonna 2020 datan määrä on 50 tsettabittiä. 2025 määrä on jo 163 tsettabittiä (Kuva 1.). Tämä on siis 163 000 miljardia gigabittiä



Kuva 1. Maailmanlaajuisen tiedon vuosittainen koko (IDC Data Age 2025, 7).

Kriittisen datan kasvu



Kuva 2. Kriittisen tiedon kokonaismäärä (IDC Data Age 2025, 10).

Samassa tutkimuksessa IDC arvioi (kuva 2), että vuoteen 2025 mennessä kaikesta maailman datasta henkilölle kriittistä on lähes 20% sekä erittäin kriittistä 10%. Kriittisellä datalla tarkoitetaan tietoa, joka on välttämätöntä henkilön päivittäisen toiminnan jatkuvuuden kannalta. Todella kriittisellä datalla sen sijaan tarkoitetaan tietoa, jolla on välittömiä ja suoria vaikutuksia henkilön terveyteen ja hyvinvointiin.

Tietosuoja-asetuksen tärkeimpänä tarkoituksena on yksilön oikeuksien parantaminen oman tiedon hallinnoinnissa. Varsinkin suurina pidettävät it-alan yritykset kuten Google, Facebook ja Apple pystyvät keräämään halutessaan valtavan määrän dataa yksilöistä, kun heidän tilejään käytetään lukemattomien palveluiden ja sovellusten yhteydessä. Ja ilman EU:n tietosuoja-asetusta, olisi näiden palveluntarjoajien tietomäärien hallinta rekisteröityneen puolesta ollut lähes mahdotonta (Meling 2018). Kiinnostavana esimerkkinä näistä em. yrityksistä Jefferson Graham kysyi huhtikuussa 2018, mitä tietoa heillä oli hänestä, ja kuinka paljon. Facebook oli taltioinut Grahamista 881 MB, Google 243 MB ja Apple ainoastaan 9 MB (Jefferson, 2018). Tämän tyyliset vertailut ja esilletulot eri palveluiden ja yritysten henkilötietokyselyistä todennäköisesti yleistyy, ja rekisteröidyt lopulta siirtyvät sellaisten yritysten ja palveluiden asiakkaiksi, jotka arvostavat rekisteröidyn oikeuksia.

2.1 Toimivallan huomattava kasvu

Luultavasti suurin muutos EU:n tietosuojasäädöksessä on entisestään huomattavasti laajennettu toimivalta. Tämä tarkoittaa sitä, että kaikki yritykset joissa käsitellään

henkilötietoja EU:n kansalaisista, ovat velvoitettuja toimimaan asetuksen vaatimalla tavalla riippumatta siitä, käsitelläänkö tietoja EU:ssa vai sen ulkopuolella. Yritykset, joiden toimipaikka on EU:n ulkopuolella ja käsittelevät EU:n kansalaisten dataa, pitää myös määrittää tietosuojavaltuutettu EU:sta (EU GDPR Portal).

Tosin tämän muutoksen kanssa olen hieman skeptinen, miten loppujen lopuksi toimivaltaa pystytään käyttämään esimerkiksi Aasian maiden yrityksiin, ja mitkä ovat seuraavat toimet hallinnollisten sakkojen maksamattomuuden jälkeen. Todennäköisesti EU pyrkii rajoittamaan yrityksen tiedonkeruuta EU:n kansalaisista, mutta nykyaikana rajoitusten kierto on tehty todella helpoksi.

2.2 Hallinnolliset seuraamukset

Hallinnollisilla seuraamuksilla tarkoitetaan sakkorangaistusta, jonka valvontaviranomainen voi määrätä tapauskohtaisesti ja olosuhteiden mukaisesti. Rangaistukseen vaikuttaa monet asiat. Hallinnollinen sakko voi olla enintään 20 000 000 euroa tai neljä prosenttia edellisen vuoden maailmanlaajuisesta liikevaihdosta riippuen siitä, kumpi vaihtoehdoista on suurempi. Hallinnollisen sakon suuruuteen vaikuttaa mm. rekisteröidyn oikeuksien rikkomisen luonne, vakavuus, kesto ja rikkomisen tahallisuus tai tuottamuksellisuus (2016/679 artikla 83).

2.3 Suostumuksen ehdot ja määritys

Suostumukseen perustuvassa tietojenkäsittelyssä on rekisterinpitäjän pystyttävä todistamaan, että rekisteröity on antanut luvan tietojensa käsittelyyn. Kirjallisessa henkilötietojen käsittelypyynnössä, jossa kirjallinen osuus koskee myös muita asioita, on pyyntö esitettävä selkeästi erillisenä ja helposti ymmärrettävänä osana. Lisäksi rekisteröidyllä on oikeus perua suostumuksensa koska tahansa. Suostumuksen poisto, eli peruuttaminen tulee olla yhtä helppoa kuin sen antaminen (2016/679 artikla 7). Tietosuoja-asetuksen mukaan suostumusta pyydettäessä alle 16 vuotiaalta, tulee vaatia vanhemman suostumus tai valtuutus. EU:n mukaan alle 16 vuotias on lapsi. Kukin jäsenvaltio voi kuitenkin omassa lainsäädännössään säätää alemmasta iästä, joka voi olla vähintään 13 vuotta (2016/679 artikla 8). Suomessa tämä raja on 13 vuotta.

Suostumus henkilön tietojen käsittelyyn pitää saada suostumusta selkeästi ilmaisevalla toimella. Tähän kelpaa kirjallinen, sähköinen tai suullinen lausuma, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu henkilötietojensa käsittelystä. Tähän riittää esimerkiksi ”rasti ruutuun” -laatikko verkkosivulla. (Meling 2018)

Tietosuoja-asetuksen mukaan suostumukseksi ei kelpaa valmiiksi rastitetut ruudut, vaikeneminen tai jonkun toimen toteuttamatta jättäminen. Suostumuksen on lisäksi katettava kaikki käsittelytoimet, jotka toteutetaan samaa tarkoitusta tai samoja tarkoituksia varten. Sähköistä pyyntöä käytettäessä suostumuksen hankintaan, pitää pyynnön olla selkeä, tiivisti esitetty eikä se saa häiritä sen palvelun käyttöä, jota varten se annetaan (2016/679 artikla 4).

2.4 Tietomurrosta ilmoittamisen velvollisuus

Rekisterinpitäjän on velvollinen ilmoittamaan henkilötietojen tietosuojaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin sisällä sen ilmitulosta valvontaviranomaiselle. Jos loukkauksesta ei todennäköisesti aiheudu riskiä rekisterissä olevien henkilöiden oikeuksille ja vapauksille, näin ei tarvitse kuitenkaan tehdä (2016/679 artikla 33).

Rekisterinpitäjä on myös velvollinen ilmoittamaan rekisteröidylle tietoturvaloukkauksesta ilman aiheetonta viivästystä, jos kyseessä oleva loukkaus aiheuttaa todennäköisesti korkean riskin henkilölle. Ilmoituksesta tulee käydä ilmi henkilötietojen tietoturvaloukkauksen luonne yksinkertaisella ja selkeällä kielellä (2016/679 artikla 34).

Henkilötietojen tietoturvaloukkauksista, niiden vaikutuksista ja korjaavista toimista on rekisterinpitäjä velvollinen pitämään dokumentointia. Tällä dokumentoinnilla valvontaviranomaisen on voitava tarkistaa, että artiklaa 33 on noudatettu (Petri Holopainen 2018, 35.).

2.5 Oikeus päästä omiin tietoihin

Tietosuoja-asetus määrittää rekisteröidylle pääsyn omiin tietoihinsa (Harjunheimo 2018). Pääsy tietoihin on hieman väärin ilmaistu. Tästä voisi ymmärtää, että pääsisi itse yrityksen serverille katsomaan omia tietojaan. Käytännössä rekisteröidyllä on pääsääntöisesti oikeus tietää henkilötietolain säännellyn tarkastusoikeuden mukaan, mitä tietoja hänestä henkilörekisteriin on tallennettu (Harjunheimo 2018).

Jotkut yritykset ovat tämän tehneet fiksusti. Monilla verkkosivuilla on palvelu, josta rekisteröity voi tilata kaiken tiedot, joka on häneen liitettävissä. Jos tällaista palvelua ei kuitenkaan löydy, on yrityksen reagoitava pyyntöön rekisteröidylle yhden kuukauden sisällä, ellei pyyntö ole monimutkainen tai niitä ei ole paljon. Tällöin aika on kaksi kuukautta. Lisäksi pyynnön toteuttamisen tulee olla rekisteröidylle maksutonta, ellei pyynnöt ole ilmeisen perusteettomia tai kohtuuttomia (Harjunheimo 2018).

2.6 Oikeus ”tulla unohdetuksi”

Jokaisella henkilöllä on oikeus ”tulla unohdetuksi” ilman aiheetonta viivytystä. Tämä tarkoittaa sitä, että rekisterinpitäjän pitää rekisteröidyn pyynnöstä poistaa häntä koskevat henkilötiedot, edellyttäen että jokin artikla 17 ehdoista täyttyy. Tällaiset pyynnöt kuitenkin voidaan evätä, jos on olemassa jokin laillinen peruste tietojen säilyttämiseen. Esimerkiksi työnantajalla on oikeus käsitellä työntekijöidensä tietoja, vaikka työntekijä sitä vastustaisikin (Petri Holopainen 2018, 16.).

2.7 Tietosuojavastaava

Tietosuoja-asetus vaatii rekisterinpitäjän ja henkilötietojen käsittelijän nimittämään tietosuojavastaavan, jos kyseessä on jokin seuraavista:

- Viranomainen tai julkishallinnon elin, joka ei ole tuomioistuin.
- Organisaatio, jonka pääasialliset tehtävät muodostuvat henkilötietojen käsittelystä, joka edellyttää laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa.

- Organisaatio, jonka pääasialliset tehtävät muodostuvat laajasta henkilötietojen käsittelystä, joka kohdistuu erityiseen henkilötietoryhmään tai rikkomuksia ja rikostuomioita koskeviin tietoihin.

Tietosuojavastaavan ensisijaisina tehtävinä on seurata henkilötietojen käsittelyn lainmukaisuutta ja edistää organisaatiossa lainsäädännön asettamien velvoitteiden toteutumista. Tietosuojavastaava toimii myös valvontaviranomaisen sekä rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa (2016/679 artiklat 37-39).

2.8 Osoitusvelvollisuus

Nykyään ei enää riitä, että yritys noudattaa tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyä, vaan yritykseltä edellytetään aiempaa tarkempaa suunnittelua, dokumentointia sekä sisäistä ohjausta henkilötietojen käsittelyssä. Tarvittaessa myös tietoja käsittelevän henkilöstön koulutusta (2016/679 artiklat 5 ja 24).

Tietosuoja-asetuksen osoitusvelvollisuuden täyttymiseksi pitää yrityksen toteuttaa useita toimenpiteitä joista osa vaatii myös dokumentoinnin. Henkilötietojen käsittelyn kuvaus yleisellä tasolla, eli seloste käsittelytoimista on kirjallinen kuvaus yrityksen suorittamasta henkilötietojen käsittelystä. Tämä on pakollinen yrityksille jotka ovat yli 250 työntekijän organisaatioita. Seloste on myös tehtävä, jos käsittely ei ole satunnaista tai aiheuttaa todennäköisen riskin rekisteröidyn oikeuksille ja vapauksille (Tietosuoja.fi 2018, seloste käsittelytoimista).

3 VAADITTAVA DOKUMENTAATIO

Dokumentoinnista ja sertifioinnista on yritykselle hyötyä kolmella tavalla. Sillä saadaan hyvä arvio organisaation nykyisestä kyberturvallisuustasosta, liiketoimintaa tehdessä sertifikaatti toimii kilpailutekijänä sekä itse arvion lopputulemasta on hyvä lähteä kehittämään heikompia aukkoja kyberturvallisuudessa (fincsc.fi 2018).

Dokumentointi myös luo uusia paineita yrityksille, koska tietosuoja-asetus velvoittaa rekisterinpitäjän osoittamaan, että käsittelylle on perusteet ja käsittely tapahtuu asetusten mukaisesti. Tämä edellyttää rekisterinpitäjältä muun muassa tarkemmin suunniteltuja ja henkilökunnalle koulutettuja prosesseja henkilötietojen käsittelyyn (ek.fi 2018).

3.1 FINCSC – Finnish Cyber Security Certificate

Sertifiointivaatimukset koostuvat arviointikohdista, jotka on jaettu yhteentoista toisiaan täydentävään kysymysalueeseen. Niillä mitataan organisaation kyberturvallisuustasoa sekä ohjataan parhaiden tietoturvakäytäntöjen valinnassa (fincsc.fi 2018). Dokumentointiin kuuluu tietoturvamenettelyohje, jossa määritellään noudatettavat tietoturvaperiaatteet yleisellä tasolla. Tietoturvamenettelyohje kattaa sekä yhteiset että työntekijän käyttöön luovutetut tietotekniset laitteet ja järjestelmät (fincsc.fi 2018).

3.2 Seloste käsittelytoimista

Seloste käsittelytoimista toimii organisaation sisäisenä asiakirjana ja osana osoitevelvollisuuden todentamista. Kyseessä on tietosuoja-asetuksen vaatima kirjallinen kuvaus yrityksen toteuttamasta henkilötietojen käsittelystä. Seloste on vapaamuotoinen, kunhan siitä käy selkeästi ilmi tarvittavat tiedot (tietosuojavaltuutetun toimisto 2018).

Yrityksellä on velvollisuus laatia seloste, jos organisaation koko on yli 250 työntekijää. Sitä pienemmän yrityksen on laadittava seloste, jos henkilötietojen käsittely aiheuttaa todennäköisen riskin rekisteröidyn oikeuksille ja vapauksille, henkilötietojen käsittely ei ole satunnaista tai rekisterissä käsitellään erityisiin tietoryhmiin kuuluvien henkilöiden tietoja, jotka koskevat rikostuomioita tai rikkomuksia (tietosuojavaltuutetun toimisto 2018).

3.3 Informointivelvoite

Tietosuoja-asetuksen mukaan rekisterinpitäjällä on informointivelvoite rekisteröidylle tietojen käsittelystä. Rekisteriselosteesta ei sen sijaan säädetä tietosuoja-asetuksessa. Tietosuoja-asetus kuitenkin velvoittaa rekisterinpitäjän arvioimaan onko selosteen kieli ymmärrettävää ja johdonmukaista kohderyhmän kannalta (tietosuojavaltuutetun toimisto 2018). Ei siis riitä, että henkilötietojen käsittelyä koskevat tiedot ovat rekisteröidyn saatavilla, vaan sen on oltava ymmärrettävässä, selkeässä ja tiiviissä muodossa. Henkilötietolain 24 § ja 10 § avulla rekisterinpitäjä on voinut laatia myös tietosuojaselosteen, joka on sisältänyt edellyttävät tiedot jo ennen asetuksen voimaantuloa. Asetuksen vaatimat dokumentit eivät ole malliltaan kovin rajoitettuja, kunhan vain vaadittavat asiat käyvät ilmi selkeästi ja ymmärrettävässä muodossa (Tietosuojavaltuutetun toimisto 2018). Tämä mahdollistaa yrityksille tilanteen erottua edukseen ja omalla tyylillään.

3.4 Käsittelyn oikeusperuste

Tietosuoja-asetus edellyttää käsittelyperustetta henkilötietojen käsittelylle. Peruste on määritettävä ennen tiedon käsittelyä ja kun perusteen mukaan on henkilötietoja kerätty, ei sitä enää voi vaihtaa toiseen. Tästä pitää myös löytyä dokumentaatio, millä perustein tietoja käsitellään (Holopainen 2018)

Tietosuoja-asetuksessa henkilötietojen käsittelyyn löytyy kuusi perustetta (Holopainen 2018, 9.):

- Rekisteröidyn suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleistä etua koskeva tehtävä tai julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Kuitenkin erityisten henkilötietoryhmien, kuten etnisen alkuperän tai terveyttä koskevan tiedon käsittely on lähtökohtaisesti kielletty ilman erillistä poikkeusta tietosuoja-asetuksessa tai kansallisessa lainsäädännössä (Holopainen 2018, 12)

3.5 Tietotilinpäätös

Tietotilinpäätös (data balance sheet) on suositeltu, mutta ei pakollinen tapa dokumentoida tiedon hallintaan ja siihen liittyviin tietoturvakäytäntöihin. Tietotilinpäätöksen tavoitteena on antaa kuvaus tietojen käsittelyn tilasta sekä arvioida tietosuojan ja -turvan toteutumista organisaatiossa. Tietotilinpäätös on osa tietojohtamista, ja yleensä käytetään organisaation sisäisenä raporttina (Haukkovaara 2017) Tietotilinpäätös auttaa hahmottamaan mitä tietovarantoja organisaatiolla on hallussa ja millainen järjestelmäarkkitehtuuri on. Lisäksi tiedon suojaus, käytön valvonta sekä tiedon käsittelyn prosessit voivat olla osa dokumentin sisältöä. Tämä auttaa valvomaan muun muassa rekisteröityjen oikeuksia tietojen hallinnassa (Meling 2018).

3.6 Yhteistyösopimukset

Tietosuoja-asetus edellyttää kirjalliset sopimukset, kun yritykset siirtävät henkilötietoja joko asiakkaistaan tai työntekijöistään muille palveluntarjoajille (Sopimustieto 2018). Tällaisia palveluntarjoajia voi olla esimerkiksi tilitoimistot ja IT-yritykset jotka ylläpitävät yrityksen tietojärjestelmiä. Rekisterinpitäjällä on vastuu käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävää tietoturvaa toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset (2016/679, artikla 28). Osoitusvelvollisuus henkilötietojen käsittelystä on loppujen lopuksi rekisterinpitäjällä. Henkilötietojen käsittelijän ja rekisterinpitäjän välisessä sopimuksessa tulee määrittää suoritettavan käsittelyn luonne, jolloin sopimus sitoo myös henkilötietojen käsittelijän käsittelemään tietoja vaaditun mukaisesti. Jos henkilötietojen käsittelijä käyttää toista henkilötietojen käsittelijää alihankintana, pitää alkuperäisen rekisterinpitäjän sopimuksessa käydä tämä myös ilmi (Kulmala 2017)

4 LOPUKSI

Tässä luvussa käyn läpi oman työskentelyni herättämät ajatukset voimaan astuvasta tietosuoja-asetuksesta, sen hyvistä puolista, epäkohdista ja haasteista. Tavoitteena opinnäytetyössä oli tehdä toimeksiantoyrityksestä laillinen rekisterinpitäjä sekä päivittää tietoturva, rekisterit sekä henkilötietojen käsittelyn prosessit ajan tasalle. Näihin kaikkiin tavoitteisiin päästiin rekisterien putsauksella ja läpikäynnillä, prosessien selkeyttämisellä, henkilökunnan koulutuksella ja mittavalla dokumentaatiolla.

4.1 Yksityishenkilönä

GDPR on hyvä uudistus yksilön ja EU:n kansalaisen kannalta. Liian pitkään yritykset ovat päässet hyötymään datasta, jota ne ovat keränneet joko luvatta tai epäselvien rekisteriselosteiden avulla. GDPR auttaa henkilöä saamaan oikeudet takaisin omaan dataansa ja sen hallintaan. Innokkaimmat oman tiedon poistajat joutuvat kuitenkin osin pettymään, sillä valtion lainsäädäntö kuitenkin ajaa EU:n asetusten edelle. Esimerkiksi Suomessa kirjanpitolaki vaatii säilyttämään tietyt dokumentit useita vuosia tapahtuman jälkeen.

4.2 Yrityksenä

Yrityksille tietosuoja-asetus on loistava rajapyykki päivittää ja yhdenmukaistaa prosessit, tietoturva sekä organisaation dokumentointi. Varsinkin liiketoiminnassa ICT-puoli on kehittynyt nopeaa vauhtia ja kaikki työkalut on pyritty ottamaan käyttöön mahdollisimman nopeasti, dokumentointiin ja tietoturvaan sen enempää paneutumatta. Rekisterien siivous on myös yksi asia jota yritykset eivät normaalisti ole suorittanut.

4.3 Haasteet yrityksenä

Pk-yritykselle uusi tietosuoja-asetus tuo paljon haasteita. Nopea siirtymäaikataulu ja selkokielisen materiaalin vähyys luo paineita, joita ilman lisäresursseja on erittäin vaikea selvittää. Monet pienet yritykset eivät edes välttämättä ymmärrä käsittelevänsä henkilötietoja.

Esimerkiksi parturikampaaja joka ottaa varauksen yhteydessä puhelinnumeron ja sukunimen hallitsee jo rekisteriä. Yleensä näitä tietoja säilytetään kassalla avoimena. Tämä tarkoittaa sitä, että aina kun kassalla asioidaan, tietoturvaloukkaus on mahdollinen.

EU on määrittänyt myös isot sanktiot määräyksien noudattamatta jättämisestä sekä säännösten rikkomisesta. Yleensä kun tietoturvaloukkaus tapahtuu, jotain on tehty väärin. Yritykset odottavat varmasti innolla tämän tyylistä ennakkotapausta ja EU tuomioistuimen linjaa siitä, mikä on riittävä tietoturva ja sen dokumentoinnin taso.

LÄHTEET

EU GDPR Portal: Key Changes with the General Data Protection Regulation (https://www.eugdpr.org/key-changes.html)

FINCSC -sertifiointi (https://www.fincsc.fi/yleista/)

Graham, Jefferson 2018. PCmag: Apple Responds to Personal Data Request with 9MB file. (https://eu.usatoday.com/story/tech/talkingtech/2018/05/04/asked-apple-everything-had-me-heres-what-got/558362002/)

Harjunheimo, Niina 2018. Elinkeinoelämän keskusliitto (https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/)

Haukkovaara, Olli 2017: Tietotilinpäätös – johtamisen työkalu, EU-vaatimusten helpottaja (https://www.tivi.fi/Kumppanit/Sofigate/tietotilinpaatos-johtamisen-tyokalu-eu-vaatimusten-helpottaja-6652925)

Holopainen, Petri 2018. Yrittäjän tietosuojaopas (https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018_130418.pdf)

IDC Data Age 2025. (https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf)

Kauremaa, Hannu 2018: GDPR & O365. Ederan järjestämä koulutus Hotel Arthurissa 8.3.2018.

Kulmala, Tatu: Lukander Ruohola HTO: Uusi tietosuoja-astus ja yritysten sopimukset (http://www.lrhto.fi/artikkelit/yrityksen-sopimukset/uusi-tietosuoja-asetus-ja-yritysten-sopimukset/)

Meling, Rami 2018. GDPR-aamiainen. GDPR-asiantuntijan luento 27.2.2018 Sokos Hotel Hamburger Börsissä.

Suomen Sopimustieto Oy 2018: Sopimus henkilötietojen käsittelystä GDPR:n mukaisesti (”DPA) (https://sopimustieto.fi/sopimus/5aPxRa-sopimus_henkilotietojen_kasittelysta_ns_gdpr_sopimus)

Tietosuoja-asetus 2016/679 (http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI)

Tietosuojavaltuutetun toimisto, käsittelytoimet (http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/selostekasittelytoimista.html)

Tietosuojavaltuutetun toimisto, Seloste käsittelytoimista (https://tietosuoja.fi/seloste-kasittelytoimista)

Tietosuojavaltuutetun toimisto, osoitusvelvollisuus (https://tietosuoja.fi/osoitusvelvollisuus)