Opinnäytetyö AMK

Tieto- ja viestintätekniikka

2018

Samuli Honkonen

EU:N TIETOSUOJA-ASETUS JA SEN VAIKUTUKSET YRITYKSEN JÄRJESTELMIIN JA KÄYTÄNTÖIHIN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2018 | 25 sivua

Samuli Honkonen

EU: N TIETOSUOJA-ASETUS JA SEN VAIKUTUKSET YRITYKSEN JÄRJESTELMIIN JA KÄYTÄNTÖIHIN

Euroopan yleisestä tietosuoja-asetuksesta päätettiin 27.04.2016 Euroopan unionin parlamentissa ja neuvostossa. Tietosuoja-asetukselle määritettiin 2 vuoden siirtymäaika, joka päättyy 25.05.2018. Yleisen tietosuoja-asetuksen tavoitteena on lisätä henkilötietojen suojaus jokaisen perusoikeudeksi sekä yhtenäistää henkilötietojen käsittelyä Euroopan unionin jäsenmaissa.

Opinnäytetyön tavoitteena on selvittää toimeksiantajan Euronic Oy:n valmius toimia yleisen tietosuoja-asetuksen alaisuudessa ja ehdottaa mahdollisia korjaustoimia. Tavoitteen saavuttaminen edellyttää tutustumista yrityksen järjestelmiin sekä käytäntöihin varsinkin henkilötietojen käsittelyn osalta. Tietosuoja-asetus vaatii myös riittävää tietoturvaa käsittelyjärjestelmille, joten työhön sisältyy myös kevyt tietoturva selvitys.

Tietosuoja-asetus määrittää, että henkilötietoja pitää käsitellä lainmukaisesti, läpinäkyvästi ja asianmukaisesti. Henkilötietojen käsittelylle pitää olla tietosuoja-asetuksen mukainen peruste ja henkilötietoja saa kerätä sekä käsitellä vain tämän perusteen vaatiman verran. Suurin tietosuoja-asetuksen tuoma muutos on osoitusvelvollisuus, joka siirtää todistustaakan henkilörekisterin ylläpitäjälle. Osoitusvelvollisuus edellyttää huomattavan määrän dokumentaatiota ja seurantaa.

Toimeksiantajan valmius on selvityksen perusteella hyvä. Henkilötietoja käsitellään turvallisesti, läpinäkyvästi ja tarkoituksenmukaisesti. Myös järjestelmien tietoturvasta on huolehdittu yrityksen oman henkilöstön toimesta. Kehitettävää yrityksellä on käsittelyn seurannassa ja dokumentaatiossa, joita vaaditaan osoittamaan, että tietosuoja-asetusta on noudatettu. Lisäksi on syytä luoda tietosuojaorganisaatio, joka huolehtii, että ehdotetut muutokset toteutetaan ja tietosuoja-asetusta noudatetaan myös tulevaisuudessa uusien järjestelmien ja mahdollisten lakimuutosten jälkeen.

ASIASANAT:

GDPR: EU:n yleinen tietosuoja-asetus; HTTPS: Suojattu internet protokolla; SSL: Suojatun yhteyden mahdollistava tietoverkon salausprotokolla; VPN: Julkisen tietoverkon yli tehtävä suojattu yhteys, joka yhdistää kaksi yksityistä tietoverkkoa

BAHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelors degree in Information technology

2018 | 25 pages

Samuli Honkonen

THE GDPR REGULATION AND ITS EFFECTS ON THE SYSTEMS AND PRACTICES OF A COMPANY

The parliament and council of the European union decided on the general data protection regulation (GDPR) on the 27th of April 2016. The regulation was given a 2-year adoption period that ends on the 25th of May 2018. The aim of the regulation is to add personal data protection as a fundamental right and to unify data processing within the European Union.

The aim of this thesis is to determine the readiness of the client Euronic Oy regarding the general data protection regulation and to suggest possible corrections for the found shortcomings. Achieving the aim requires examining the systems and practices of the company regarding the handling of personal data. The regulation also requires the information security of the company to be at an acceptable level which requires an information security investigation.

The general data protection regulation requires that personal data is handled transparently, lawfully and fairly. The processing of personal data needs to be based on an accepted purpose and the data can be handled and collected only for that purpose. The biggest change brought by the regulation is the accountability of the data processor that requires comprehensive documentation and monitoring of personal data processing.

Based on the investigation the readiness of the client is at good level. The processing of personal data is safe, transparent and appropriate. The information security of the processing systems is taken care of by the personnel of the company. The shortcomings of the company are the documentation and monitoring of the personal data processing that are required to fill the accountability requirement. Additionally, the client should create a data protection organization that is responsible for implementing the suggested changes and to make sure the general data protection regulation is complied with in the future.

KEYWORDS:

GDPR: General data protection regulation; HTTPS: Secured internet protocol; SSL: An encryption protocol for data transfer; VPN: Virtual private network that is used to create a secure connection over the internet

SISÄLTÖ

1 JOHDANTO

Euroopan parlamentti ja Euroopan unionin neuvosto päätti 27.4.2016 yleisestä tietosuoja-asetuksesta (GDPR 2016/679). Asetus tuli voimaan välittömästi ja sen soveltaminen aloitetaan 25.5.2018 kahden vuoden siirtymäajan jälkeen. Tietosuoja-asetuksen tavoitteena on yhtenäistää ja tiukentaa henkilötietojen käsittelyyn liittyviä vaatimuksia Euroopan unionin jäsenvaltioissa.

Opinnäytetyön tavoitteena on selvittää toimeksiantajan Euronic Oy:n valmius tietosuoja-asetuksen soveltamiseen ja tuoda esille mahdolliset puutteet. Tavoitteeseen pääseminen vaatii tietosuoja-asetuksen sisältöön ja yrityksen järjestelmiin sekä käytäntöihin tutustumista. Selvitystyön jälkeen dokumentoidaan miltä osin yrityksen järjestelmät ja käytännöt täyttävät tietosuoja-asetuksen vaatimukset sekä mitä mahdollisia puutteita henkilötietojen käsittelyssä on ja miten ne tuodaan vaatimusten tasolle.

Lähdeaineistona työssä käytetään pääasiassa tietosuoja-asetuksen virallista tekstiä ja siitä tehtyjä asiantuntijoiden tulkintoja. Virallinen teksti on hyvin yleistävä, joten se on myös hyvin tulkinnanvarainen jokaisen toimijan kohdalla. Koska tietosuoja-asetusta ei sovelleta vielä, siitä ei ole ennakkotapauksia, joista selviäisi enemmän käytännön toteutusta.

Työssä käydään tietosuoja-asetus läpi loogisessa järjestyksessä keskittyen toimeksiantajayritykseen vaikuttaviin kohtiin, määritetään jokaisen kohdan aiheuttamat vaikutukset ja verrataan niitä yrityksen henkilötietojen käsittelyn nykytilaan. Opinnäytetyö on tehty nimenomaan toimeksiantajan näkökulmasta, joten työ ei anna täydellistä kuvausta tietosuoja-asetuksesta eikä työtä voi käyttää suoraan eri toimijoiden vaikutustenarvioinnissa.

Suomen lainsäädäntö on kattanut jo pitkän aikaa suuren osan tietosuoja-asetuksen vaatimuksista, joten lähtöoletuksena on, että yrityksen järjestelmät ja käytännöt täyttävät myös tietosuoja-asetuksen vaatimukset suurilta osin. Vaikka työn lopputuloksena olisi, että yritys täyttää tietosuoja-asetuksen täysimääräisenä yritykselle jää vaadittu dokumentaatio, joka osoittaa, että tietosuoja-asetusta noudatetaan.

2 EU:N LAAJUINEN TIETOSUOJA-ASETUS

Miksi Euroopan unionin komissio katsoi tarpeelliseksi luoda koko unionin laajuisen tietosuoja-asetuksen? Virallisesti syiksi määritellään muun muassa henkilötietojen suojauksen perusoikeus, Euroopan unionin sisämarkkinoiden yhdentyminen ja teknologian jatkuvan kehityksen aiheuttamat haasteet. (Yleinen tietosuoja-asetus 2016, alkumääritelmät) Yleisellä tietosuoja-asetuksella siis varmistetaan, että kaikkien Euroopan unionin kansalaisten henkilötietoja käsitellään riittävän turvallisesti. Turvallisuuden lisäksi asetus helpottaa useissa maissa toimivia yrityksiä, sillä jatkossa niiden on noudatettava vain yleistä tietosuoja-asetusta jokaisen eri maan lainsäädännön sijaan ja lisäksi heidän tarvitsee raportoida vain yhden jäsenvaltion tietosuojaviranomaiselle. (Oikeusministeriö 2017) Tietosuoja-asetus luo henkilötietojen turvalliselle käsittelylle pohjan, jota voidaan tarvittaessa täydentää kansallisella lainsäädännöllä. (Tietosuojavaltuutetun toimisto 2015)

Teknologian nopean kehityksen mukana pysyminen on suurempi haaste. Henkilötietoja on käsitelty ja myös tullaan käsittelemään tavoilla, joita ei voida aina ennustaa. Esimerkiksi sosiaalinen media on muuttanut henkilötietojen saatavuutta ja käsittelyä huomattavasti. Tästä syystä tietosuoja-asetus asettaa henkilötietojen käsittelylle ehtoja, kuten henkilötietojen luvanvarainen ja läpinäkyvä käsittely, jotta henkilö itse pystyy seuraamaan ja päättämään henkilötietojensa käsittelystä. Tämän lisäksi teknologian kehityksestä vastaaville toimijoille määrätään enemmän vastuuta kehittämästään teknologiastaan, pakottamalla heidät dokumentoimaan kehitystä ja ottamaan tietosuoja osaksi kehitysprosessia tuntuvien sakkojen uhalla. (Yleinen tietosuoja-asetus 2016, luku 2)

Huomionarvoista on, että Euroopan unionin yleinen tietosuoja-asetus kattaa kaikkien unionin jäsenmaiden kansalaisten ja unionin alueella oleskelevien henkilötiedot riippumatta siitä missä maassa henkilötietoja käsitellään. Käytännössä siis asetusta sovelletaan globaalisti, sillä Euroopan unionin markkinoiden ulkopuolelle jääminen on lähes mahdottomuus globaalissa taloudessa. Euroopan unionin komissio pitää kirjaa verkkosivuillaan maista, joiden tietosuoja on katsottu riittäväksi. Jos henkilötietoja siirretään maihin, joita komissio ei ole määrittänyt turvallisiksi, siirron ja käsittelyn turvallisuus pitää varmistaa ja vahvistaa kirjallisella sopimuksella, jolla kompensoidaan maan puutteellista tietosuojaa. (Valtiovarainministeriö 2016)

Voidaan myös spekuloida, että tietosuoja-asetus on vastaus suurien teknologiayrityksen mielivaltaiselle henkilötietojen suorastaan hyväksikäytölle omiin tarkoituksiinsa. Tästä antaa viitteitä tietosuoja-asetuksen kattavuus kaikille Euroopan unionin kansalaisille riippumatta heidän nykyisestä olinpaikastaan sekä käsittelyn luvan vaatiminen rekisteröidyltä jokaiselle käsittelytarkoitukselle erikseen. Tietosuoja-asetuksella halutaan siis myös avata itse käsittelyn alla olevien henkilöiden silmät ja antaa heille mahdollisuus vaikuttaa käsittelyyn. Koko unionin laajuisena tietosuoja-asetuksella on myös riittävästi vaikutusvaltaa takana saadakseen mielivaltaisen käsittelyn loppumaan.

Tietosuoja-asetus on myös nimensä mukaisesti asetus. Asetukset ovat Euroopan unionin säädöksistä vaikutusvaltaisimpia ja ovat verrattavissa kansallisiin lakeihin. Asetukset ovat aina sitovia kaikille Euroopan unionin jäsenvaltioille ja niitä säädetään vain oikean tarpeen edessä. Tästä voidaan tulkita, että Euroopan unioni on huolissaan henkilötietojen käsittelyn nykytilasta ja haluaa kaikki jäsenvaltiot korjaustoimenpiteisiin.

3 YLEISET SÄÄNNÖKSET

Tietosuoja-asetuksen ensimmäisessä luvussa määritetään asetuksen kohteet ja tavoitteet, soveltamisalat sekä tuodaan esille määritelmät. Näiden määritysten perusteella tiedetään paremmin mitä ja ketä asetus koskee. Tiivistettynä tietosuoja-asetuksen tavoitteena on tehdä henkilötietojen suojauksesta perusoikeus Euroopan Unionin kansalaisille sekä taata heille kaikki oikeudet ja vapaudet omiin henkilötietoihinsa. (Yleinen tietosuoja-asetus 2016, luku 1)

3.1 Asetuksen soveltaminen

Asetusta sovelletaan toimeksiantaja yritykseen, sillä yrityksen liiketoiminta edellyttää, että asiakkaista ja henkilökunnasta pidetään henkilörekistereitä eli yritys on rekisterinpitäjä ja henkilötietojen käsittelijä. Suomalaisena yrityksenä käsiteltävät henkilötiedot kuuluvat lähes poikkeuksetta EU:n kansalaisille.

3.2 Määritelmät

Koska toimeksiantaja yritys käsittelee hyvin rajattua määrää henkilötietoja eikä analysoi niitä, suuri osa määritelmistä, jotka koskevat profilointia, terveystietoja ja monikansallisia konserneja, voidaan ohittaa yritystä koskemattomana.

Tietosuoja-asetuksessa henkilötiedoilla tarkoitetaan mitä tahansa tietoa, jolla voidaan tunnistaa yksittäinen henkilö. Toimeksiantajan tapauksessa nämä tiedot ovat yleiset henkilötiedot, kuten nimi, ja yhteystiedot, kuten osoite, puhelinnumero ja sähköpostiosoite. Tämän lisäksi tietotekniikan palveluita tarjoavana yrityksenä käsiteltävänä on myös vähemmän tunnettuja henkilötietoja, kuten palvelun käyttäjätunnus ja asiakkaalle annettu julkinen IP-osoite, joita on käsiteltävä samoin kuin yleisiä henkilötietoja. (Yleinen tietosuoja-asetus 2016, luku 1)

Henkilötietojen käsittelyllä tarkoitetaan mitä tahansa henkilötietoihin kohdistuvaa manuaalista tai automaattista toimintaa. Toimeksiantajan käsittely keskittyy palveluiden tarjoamiseen. Käytännössä henkilötietojen käsittely on siis tietojen tallennusta, päivitystä,

käyttöä palvelun tarjontaan ja lopulta poistoa asiakassuhteen päättymisen jälkeen. Käsittely tapahtuu henkilötietojen käsittelijän toimesta, joka on yrityksen työntekijä tai kolmas osapuoli, jolle henkilötietojen käsittelyä on ulkoistettu. (Yleinen tietosuoja-asetus 2016, luku 1)

Rekisterillä tarkoitetaan jäsenneltyä joukkoa henkilötietoja, josta on mahdollista saada tietoja ulos. Rekisterin määritelmä on siis hyvin yleinen, joka tarkoittaa, että henkilörekisterin määritelmän täyttää kaikki järjestelmät, jonne on merkitty edes kahden henkilön tiedot. Tällä menetelmällä pyritään tukkimaan kaikki mahdolliset porsaanreiät asetuksessa. Tyypillisiä henkilörekistereitä ovat asiakas-, henkilökunta- ja jäsenrekisterit. Rekisterit voivat olla esimerkiksi mappeja, SQL-tietokantoja tai Excel-tauluja. (Yleinen tietosuoja-asetus 2016, luku 1)

4 PERIAATTEET

Tietosuoja-asetuksen toinen luku määrittää miten ja millä periaatteilla henkilötietoja saa käsitellä. Periaatteiden noudattaminen on pystyttävä osoittamaan rekisterinpitäjän osalta esimerkiksi kattavalla dokumentaatiolla. Tätä kutsutaan tietosuoja-asetuksessa osoitusvelvollisuudeksi. Tietosuoja-asetus on siis hyvin poikkeava yleisistä oikeusperiaatteista, sillä todistustaakka siirretään syytetylle. (Yleinen tietosuoja-asetus 2016, luku 2)

4.1 Tietosuoja-asetuksen yleiset periaatteet

Käsittelyn lähtökohta on, että henkilötietoja käsitellään lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Tämä tarkoittaa, että henkilötietoja voi kerätä vain tiettyä määritettyä tarkoitusta varten ja vain tämän tarkoituksen vaatiman verran. Henkilötietojen säilytyksen osalta tietojen pitää olla täsmällisiä, rajoitettuja ja eheitä. Säilytys pitää siis tapahtua tietoturvallisesti ja tietoihin pääsy on oltava rajoitettu vain käsittelyn kannalta tarpeellisille henkilöille. (Yleinen tietosuoja-asetus 2016, luku 2)

Tietosuoja-asetus myös määrittää, että rekisteröity saa olla tunnistettavissa tiedoistaan vain niin kauan kuin pääasiallinen käsittely sitä vaatii. Tämä on osittain ristiriidassa esimerkiksi Suomen kirjanpitolain kanssa, joka edellyttää, että kirjanpitoa säilytetään toimialasta riippuen 5–10 vuotta. Ristiriita on kuitenkin huomioitu tietosuoja-asetuksessa määrittämällä, että henkilötietoja voidaan säilyttää pidempään, jos yleinen etu sitä vaatii. Käsittelyn jälkeen henkilötietoja voidaan säilyttää vain, jos niistä ei pysty tunnistamaan rekisteröityä esimerkiksi anonymisoimalla tiedot. Tämä voidaan toteuttaa säilyttämällä vain henkilötiedot, joita ei pysty liittämään tiettyyn henkilöön, kuten ikä, pituus tai sukupuoli. (Yleinen tietosuoja-asetus 2016, luku 2)

Tietosuoja-asetuksen yhteydessä henkilötietojen suojaikärajaksi määritetään 16 vuotta. Alle 16 vuotiaiden henkilöiden henkilötietojen käsittely vaatii käsiteltävän vanhemman tai vanhempaan verrattavan suostumuksen. (Yleinen tietosuoja-asetus 2016) Varsinkin digitaalisesti henkilötietoja kerättäessä vanhemman suostumuksen saaminen on hyvin haasteellista, sillä perhesuhteita on vaikea selvittää ja varmentaa. Useat yritykset saattavat tästä syystä harkita palveluiden tarjoamista vain yli 16 vuotiaille. Tätä rajaa voidaan laskea kansallisesti 13 vuoteen. (Yleinen tietosuoja-asetus 2016, luku 2)

Suuri osa yleisistä periaatteista koskee erityisiä henkilötietoja, kuten biometrisiä, mielipiteellisiä sekä vakaumuksellisia tietoja. Näiden käsittelyä on rajoitettu erityisen tiukasti. Toimeksiantaja ei käsittele erityiseksi määriteltyjä henkilötietoja, joten niiden osalta periaatteet voidaan sivuuttaa.

4.2 Toimeksiantajan valmius

Toimeksiantajan tapauksessa tietosuojan tarve alkaa asiakassuhteeseen perustuvasta henkilötietojen käsittelystä. Henkilötietoja kerätään jo nyt minimaalinen määrä, jolla voidaan tunnistaa asiakas sekä ylläpitää asiakassuhdetta ja palveluita. Henkilötietoja säilytetään omissa järjestelmissä, jotka sijaitsevat yrityksen omassa palvelinsalissa. Täten voidaan varmistaa, että henkilötietoihin pääsee käsiksi vain yrityksen oma henkilöstö. Tämän lisäksi täsmällisyys ja eheys on helpompi varmistaa keräämällä lokitiedostoja ja tallentamalla varmuuskopioita. Myös järjestelmien tietoturvallisuus on täysin yrityksen itsensä hallinnassa. Yrityksen henkilöstöllä on valmiudet ja riittävä ammattitaito varmistaakseen, että tietosuoja-asetuksen yleiset periaatteet täyttyvät.

4.3 Kehitysehdotukset

Kehitettävää toimeksiantajalla on henkilötietojen poistossa ja arkistoimisessa käsittelyn päätyttyä. Ehdotuksena on luoda jokin järjestelmä, jolla seurataan poistuneita asiakkaita, jonka henkilötietojen käsittelylle ei ole enää perusteita. Poistuneiden asiakkaiden tiedot pitää poistaa asiakassopimuksessa määritetyn ajan jälkeen ja arkistoida tiedot kuten kirjanpito, jotka lain mukaan pitää säilyttää kauemmin. Suosituksena olisi, että järjestelmä olisi automaattinen suuren asiakaskunnan ja inhimillisten virheiden vähentämisen seurauksena. Arkistoidut tiedot pitäisi rajata vain tiettyjen avainhenkilöiden saataville.

Henkilöstön suorittamalle henkilötietojen käsittelylle pitää luoda tarkemmat käytännöt, jotka määrittävät, miten ja millä perusteella henkilötietoja käsitellään. Tällä hetkellä käsittely on turvallista, mutta hieman vaihtelevaa käsittelijöiden välillä. Dokumentoidut käytännöt yhdenmukaistavat käsittelyä ja samalla osoittavat, että käsittely on tietosuoja-asetuksen vaatimalla tasolla. Tämä myös helpottaa käsittelijöiden työtaakkaa, sillä sovittuihin käytäntöihin pystyy tukeutumaan epävarmoissa tilanteissa.

Lokitiedostoja on syytä kerätä ja tallentaa yhä enemmän. Lokeista pitäisi selvitä vähintään ketä on käsitellyt, mitä on käsitelty ja koska on käsitelty. Lokitiedostojen kerääminen on tärkeä osa osoitusvelvollisuutta. Myös yleisien järjestelmänvalvoja tunnusten käyttö on suositeltavaa lopettaa, sillä kirjautunutta henkilöä on haastavaa todentaa.

Palveluiden tarjoamista vain yli 16 vuotiaille kannattaa harkita, sillä alaikäisen henkilötietojen käsittely vaatii käsiteltävän vanhemman suostumuksen. Tämän toteuttaminen on haasteellista varsinkin digitaalisten palveluiden tarjonnassa.

5 REKISTERÖIDYN OIKEUDET

Tietosuoja-asetuksessa rekisteröidyllä on huomattava määrä oikeuksia, jotka mahdollistavat omien henkilötietojen seurannan, hallinnan ja poiston. Tarkoituksena on tehdä henkilötietojen käsittelystä mahdollisimman läpinäkyvää rekisteröidylle itselleen. (Yleinen tietosuoja-asetus 2016, luku 3)

5.1 Henkilötietojen keräys ja seuranta

Henkilötietojen keräyksen yhteydessä on ilmoitettava yksityiskohtaisesti mihin henkilötietoja käytetään, millä perusteella niitä kerätään sekä kuka käsittelee niitä ja kenelle niitä luovutetaan. Näiden lisäksi on syytä ilmoittaa rekisterinpitäjän edustajan yhteystiedot. Rekisteröidylle on myös ilmoitettava, jos hänen henkilötietoja kerätään muualta kuin häneltä itseltään. (Yleinen tietosuoja-asetus 2016, luku 3)

Rekisteröidyllä on myös oikeus päästä seuraamaan omia tietojaan. Omien henkilötietojensa lisäksi oikeus koskee myös käsittelyn yhteydessä kertynyttä tietoa. Oikeus koskee kaikkea henkilöön liittyvää tietoa, joten on syytä varmistaa, että tiedot ovat oikeat eikä sisällä mitään ylimääräistä. Rekisteröidyllä on samalla oikeus oikaista tiedot, jos niistä löytyy epätarkkuuksia tai virheellisyyksiä. Epätarkkuuksiin voi toimittaa lisäselvennyksiä ja virheelliset tiedot voi oikaista. (Yleinen tietosuoja-asetus 2016, luku 3)

5.2 Oikeus tulla unohdetuksi

Tietosuoja-asetuksen seurauksena rekisteröidyllä on oikeus tietojensa poistoon, joka tunnetaan yleisemmin oikeutena tulla unohdetuksi. Käytännössä oikeus tarkoittaa, että rekisteröidyn pyynnöstä rekisterinpitäjän täytyy poistaa tai anonymisoida henkilötiedot niin, että alkuperäinen henkilö ei ole enää tunnistettavissa. Oikeutta ei sovelleta, jos henkilötietoja käytetään julkisen vallan käyttämiseen, yleisen edun mukaiseen tarkoitukseen tai sananvapautta koskevan oikeuden täyttämiseen. Suurimmalle osalle yksityisistä toimijoista kirjanpitolaki on ainoa, joka edellyttää henkilötietojen säilyttämisen, vaikka rekisteröity on käyttänyt oikeuttaan tietojen poistoon. (Yleinen tietosuoja-asetus 2016, luku 3)

Vaikka itse oikeus on yksinkertainen se edellyttää huomattavan suuria toimenpiteitä suuremmissa yrityksissä. Henkilötiedot saattavat olla hajautettuna useisiin eri järjestelmiin, joita on varmuuskopioitu moneen otteeseen. Tämä tekee henkilötietojen poistoprosessista hyvin työlään. Kuitenkin tietosuoja-asetus on hyvin tulkinnanvarainen kokonaisuudessaan, joten tässä tapauksessa voidaan tulkita, että varmuuskopiot ovat riittävän rajoitettuja, joten henkilötietoja ei tarvitse erikseen poistaa niistä. Normaalitilanteessa varmuuskopiot tuhotaan, kun niiden sisältämä tieto vanhenee. Ongelmaksi muodostuu varmuuskopion palautus tuotantojärjestelmään ongelmatilanteessa. Tässä tapauksessa jo poistetut tiedot pitää poistaa uudestaan eli poisto-oikeutta käyttäneet henkilöt pitää listata, mutta rekisteröityä ei saa tunnistaa listalta. Rekisteröidyistä voi siis tallentaa esimerkiksi asiakasnumeron tai vastaavan numerosarjan, joka on oleellinen vain yrityksen omassa järjestelmässä.

5.3 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada hänen toimittamat henkilötiedot rekisterinpitäjältä. Henkilötiedot on toimitettava yleisesti käytetyssä ja koneellisesti luettavassa muodossa, joka tarkoittaa esimerkiksi tekstitiedostoa (.txt) tai taulukkotiedostoa (.xml), joita voidaan lukea oletuksena monilla käyttöjärjestelmillä ja ohjelmilla. Rekisteröity voi myös pyytää rekisterinpitäjää siirtämään tiedot suoraan uudelle rekisterinpitäjälle. (Yleinen tietosuoja-asetus 2016)

Kaikista yksinkertaisin tapa on toteuttaa tietojen siirto käsin, jossa tiedot kirjataan henkilötietojen käsittelijän toimesta. Jos säilytettävien henkilötietojen määrä on suuri ja oletuksena on, että pyyntöjä tulee usein, on suositeltavaa harkita automaattisesta järjestelmää, joka kerää rekisteröidyn tiedot ja toimittaa ne hänelle.

5.4 Toimeksiantajan valmius

Yksinkertaisimmillaan rekisteröidyn oikeuksien toteuttaminen vaatii luotettavaa kommunikoinnin kanavaa rekisteröidyn ja rekisterinpitäjän välillä, läpinäkyvyyttä henkilötietojen käsittelyssä sekä luotuja käytäntöjä henkilötietojen poistolle ja siirrolle. Näiden vaatimusten perusteella toimeksiantajan valmius on jo hyvä lukuun ottamatta dokumentoituja

sekä vakiintuneita käytäntöjä. Yrityksen asiakkailla on hyvin tiedossa, mihin heidän henkilötietojaan käytetään, ja heillä on mahdollisuus päivittää sekä seurata tietojaan useita eri kanavia käyttäen.

5.5 Kehitysehdotukset

Selvityksen perusteella toimeksiantajan valmius rekisteröidyn oikeuksien täyttämiselle on hyvä, joten suoranaisia muutoksia ei ole tarpeen tehdä. Suurin kehitettävä osa-alue on dokumentaatio ja käytänteet, joita on tarpeen lisätä, jotta tietosuoja-asetuksen vaatima osoitusvelvollisuus täyttyy ja mahdolliset epäselvyydet käsittelyssä vähenevät. Dokumentaatiosta pitää selvitä, minne henkilötietoja on tallennettu ja jaettu, jotta voidaan varmistaa, että henkilötiedot täsmäävät kaikissa rekistereissä. Rekisteröidyn käyttäessä poisto-oikeuttaan dokumentaatiosta voidaan varmistaa, että kaikki rekisteröidyn tiedot ovat poistettu kaikista rekistereistä. Kaikille rekisteröidyn pyynnöille on syytä luoda käytännöt, joita noudatetaan tarkkaan. Tämä vähentää huomattavasti mahdollisia virheitä pyyntöjen käsittelyssä. Pyyntöjen vaatimia toimenpiteitä on mahdollista automatisoida esimerkiksi kehittämällä asiakkaille mahdollisuus ladata omat henkilötietonsa suoraan tekstitiedostona.

6 YLEISET VELVOLLISUUDET

Tietosuoja-asetus määrittää rekisterinpitäjille ja henkilötietojen käsittelijöille yleisiä velvollisuuksia, jotka pitää täyttää ennen henkilötietojen käsittelyn aloittamista. Velvollisuudet ovat riskilähtöisiä ja niiden vaativuus suhteutetaan rekisterinpitäjän saatavilla oleviin resursseihin, jotta tietosuoja-asetus ei aiheuttaisi suhteettoman suurta taloudellista painetta pienyrityksille, yhdistyksille ja seuroille. (Yleinen tietosuoja-asetus 2016, luku 4)

Rekisterinpitäjällä on vastuu varmistaa ja osoittaa, että henkilötietojen käsittely noudattaa tietosuoja-asetusta. Käytännössä osoitus tapahtuu laajalla käsittelyn dokumentaatiolla ja seurannalla, joita pitää tarkistaa ja päivittää tarvittaessa. Henkilötietojen käsittelylle voi myös harkita ulkopuolisen tahon tekemää sertifiointia. (Yleinen tietosuoja-asetus 2016, luku 4)

Sisäänrakennettu ja oletusarvoinen tietosuoja toteutetaan varmistamalla, että luvun 3 ja 4 mukaiset tietosuojaperiaatteet sekä rekisteröidyn oikeudet toteutuvat päivittäisessä käsittelyssä. Sisäänrakennettu ja oletusarvoinen tietosuoja voidaan myös sertifioida osoituksena, että sitä noudatetaan. (Yleinen tietosuoja-asetus 2016, luku 4)

6.1 Henkilötietojen käsittelijä

Tietosuoja-asetus määrittää myös yleisiä velvollisuuksia henkilötietojen käsittelijöille, jotka voivat olla suoraan rekisterinpitäjän palveluksessa tai ulkoistettuja käsittelijöitä. Rekisterinpitäjä saa käyttää vain käsittelijöitä, jotka noudattavat tietosuoja-asetusta. (Yleinen tietosuoja-asetus 2016, luku 4)

Henkilötietojen käsittely on määritettävä sopimuksella rekisterinpitäjän ja käsittelijän välillä. Sopimuksessa määritetään käsittelyn luonne ja tarkoitus sekä sovitaan osapuolien velvollisuudesta henkilötietojen tietosuojasta. Henkilötietojen käsittely ei saa poiketa sovitusta. Sopimuksen vastainen käsittely tekee käsittelijästä tietosuoja-asetuksen mukaan rekisterinpitäjän. (Yleinen tietosuoja-asetus 2016, luku 4)

Rekisterinpitäjän alaisuudessa toimivat käsittelijät toimivat yleensä työsopimuksen tai muun vastaavan sopimuksen alaisena. Kyseiseen sopimukseen on syytä lisätä vaitiolosopimus liitteeksi. Vaitiolosopimuksesta tulee siis viimeistään tietosuoja-asetuksen

myötä standardi kaikilla aloilla, sillä lähes kaikilla työntekijöillä on pääsy johonkin henkilörekisteriin.

6.2 Seloste käsittelytoimista

Jokaisen rekisterinpitäjän on ylläpidettävä selostetta omista henkilötietojen käsittelytoimistaan. Selosteesta on selvittävä ainakin henkilötietojen säilytysaika, rekisterinpitäjän yhteystiedot, käsittelyn tarkoitukset, henkilötietojen vastaanottajat ja kuvaus henkilötietojen turvallisuudesta. Selosteen tapauksessa enemmän tietoa on parempi, sillä dokumentaatiolla varmistetaan, että osoitusvelvollisuus on toteutunut. Selosteen ei tarvitse olla julkinen, mutta se on luovutettava pyydettäessä valvontaviranomaiselle. Tietysti läpinäkyvyyden kannalta ainakin osa selosteesta on suositeltava julkistaa. (Yleinen tietosuoja-asetus 2016, luku 4)

Tietosuoja-asetus osoittaa taas epäselvyytensä määrittämällä, että selostevaatimukset eivät koske alle 250 työntekijän yrityksiä tai järjestöjä ellei niiden käsittely ole säännöllistä tai aiheuta mahdollista riskiä rekisteröidylle. Käytännössä kaikkien yritysten henkilötietojen käsittely on säännöllistä asiakas- ja työntekijärekistereissä, joten seloste on pakollinen kaikille rekisterinpitäjille. Lisäksi riski on aina olemassa, kun henkilötietoja tallennetaan ja käsitellään. (Yleinen tietosuoja-asetus 2016, luku 4)

6.3 Henkilötietojen turvallisuus

Tietosuoja-asetus määrittää rekisterinpitäjille toimia, joilla vähennetään riskiä henkilötietojen vaarantumisesta. Tämän lisäksi rekisterinpitäjillä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta sekä viranomaisille että rekisteröidyille.

6.3.1 Käsittelyn turvallisuus

Käsittelyn turvallisuus on hyvin pieni osa itse tietosuoja-asetusta, mutta se on myös työläin sekä vaatii eniten dokumentaatiota. Käsittelyn turvallisuus tarkoittaa järjestelmien yleistä tietoturvaa, vikasietoisuutta, eheyttä ja käytettävyyttä. Varsinkin opinnäytetyön

toimeksiantajan tapauksessa kyseinen kohta tietosuoja-asetuksesta on vaativa, sillä yrityksellä on oma datakeskus, joka sisältää huomattavan määrän eri laitteita ja järjestelmiä, joiden tietoturva on varmistettava.

Tietoturvallisuuden varmistaminen on monen tekijän summa, sillä tietoturva toimii heikoimman lenkin periaatteella. Järjestelmien vaarantuminen vaatii usein vain yhden haavoittuvuuden käyttöä. Tietosuoja-asetus ei määritä tarkalleen, mitä toimia tietoturvan varmistaminen vaatii, joten varmistamiseen vaadittujen toimien selvittäminen jää rekisterinpitäjien vastuulle. Tietosuoja-asetuksessa rekisterinpitäjältä vaaditut toimet suhteutetaan toimijan resursseihin, käsittelyn luonteeseen ja henkilötietojen vaarantumisen riskiin. Tietoturvan takaaminen vaatii minimissään ajan tasalla pidettävät järjestelmät, pääsynhallinnan sekä palomuurien ja virustorjuntojen käytön. (Valtiovarainministeriö 2016)

Henkilötiedot on oltava suojattuna koko elinkaarensa ajan, joten ne on myös kuljetettava ja kerättävä suojattuja kanavia pitkin. Kaikki internetsivustot, jotka keräävät henkilötietoja esimerkiksi lomakkeella, vaativat suojatun https -yhteyden käyttöä, jolla varmistetaan turvallinen henkilötietojen siirto. Myös kaikki käsittelyn aikana tapahtuva siirto on tehtävä käyttäen suojattuja yhteyksiä. Huomattavaa on, että esimerkiksi vpn -yhteydellä henkilötietojen käsittely rinnastetaan henkilötietojen siirtoon siihen valtioon, josta yhteys on muodostettu. (Yleinen tietosuoja-asetus 2016, luku 4)

Käsittelyn turvallisuus vaatii myös käsittelyjärjestelmiltä vikasietoisuutta ja eheyttä. Vikatilanteessä järjestelmät on pystyttävä normalisoimaan nopeasti ja eheys vikatilannetta edeltävään hetkeen on säilytettävä. Järjestelmiä on siis syytä varmuuskopioida riittävästi ja tämän lisäksi harjoitella vikatilanteesta palautumista. (Valtiovarainministeriö 2016)

Tietosuoja-asetus vaatii, että rekisterinpitäjät luovat menettelyn, jolla testataan, tutkitaan ja arvioidaan säännöllisesti tietojenkäsittelyn turvallisuutta. Tämä tarkoittaa, että tietosuoja otetaan osaksi päivittäistä työskentelyä uusien järjestelmien luonnissa ja vanhojen ylläpidossa. Tietosuojasta vastuussa olevien henkilöiden on syytä kokoontua tietosuojavastaavan johtamana useamman kerran vuodessa ja arvioida tietojenkäsittelyn nykytilan. Samalla voidaan varmistaa, että henkilötietojen käsittelyn ohjeet ovat ajan tasalla ja henkilötietojen käsittelijät noudattavat ohjeistusta. (Valtiovarainministeriö 2016)

6.3.2 Ilmoitus tietoturvaloukkauksesta

Tietosuoja-asetus määrittää, että henkilötietojen tietoturvaloukkauksista on ilmoitettava valvontaviranomaiselle 72 tunnin kuluessa loukkauksen tiedostamisesta. Ilmoitusta ei tarvitse tehdä, jos loukkauksesta ei todennäköisesti aiheudu riskiä rekisteröidylle. Ilmoituksesta on selvittävä loukkauksen luonne, laajuus ja mahdolliset seuraukset. Tämän lisäksi ilmoitukseen on sisällytettävä tietosuojavastaavan yhteystiedot sekä rekisterinpitäjän ehdotetut tai jo toteutetut toimenpiteet varmistaakseen, ettei loukkaus toistu ja mahdollisten haittavaikutusten lieventämiseksi. Rekisteröidyille loukkauksesta pitää ilmoittaa vain, jos loukkaus aiheuttaa korkean riskin rekisteröidyn oikeuksille tai vapauksille. Kaikki tietosuojaloukkaukset on dokumentoitava, jotta viranomainen voi tarkistaa, että artiklaa on noudatettu. (Valtiovarainministeriö 2016)

6.4 Toimeksiantajan valmius

Suomessa kunnioitus henkilötietoja kohtaan on yleisesti hyvällä tasolla ja toimeksiantaja ei tee tähän poikkeusta. Henkilötietojen käsittely tapahtuu turvallisesti ja sovitun mukaisesti sekä pääosin omien työntekijöiden toimesta. Ohjeistus käsittelystä on kattavaa ja turvallista, joskin pääosin suullista. Henkilötietojen käsittely siis noudattaa nyt jo tietosuoja-asetusta. Dokumentaation ja kirjallisen ohjeistuksen määrä on vähäistä.

Yrityksellä on jo olemassa henkilötietojen käsittelystä julkinen seloste, joka täyttää pääosin tietosuoja-asetuksen vaatimukset. Selosteesta selviää kerätyt henkilötiedot, henkilötietojen käyttötarkoitus sekä yhteystiedot henkilötiedoista vastaavalle.

Käsittelyn turvallisuus on lähtö-oletuksen mukaisesti hyvällä tasolla. Yrityksen koko liiketoiminta pohjautuu yrityksen omaan datakeskukseen, jonka kulmakiviä ovat tietoturva, vikasietoisuus ja eheys. Henkilötietojen säilytys ja käsittely tapahtuvat omassa datakeskuksessa, jonka järjestelmin pääsy on rajoitettu sekä sähköisesti, että fyysisesti. Sähköinen pääsy on rajoitettu vain yrityksen sisäverkkoon ja kirjautuminen vaatii aina tunnistautumisen. Yrityksen laitteisto on palomuurien ja virustorjuntojen suojaamaa. Fyysinen turvallisuus on taattu useilla lukituilla ovilla, valvontakameroilla sekä hälytysjärjestelmällä. Vikasietoisuus on varmistettu kahdentamalla lähes kaikki järjestelmät ja infrastruktuuri sekä käyttämällä datakeskuksiin tarkoitettua vikasietoista tekniikkaa. Katta-

valla varmuuskopioinnilla varmistetaan järjestelmien eheys vikatilanteesta palautumisessa. Kaikki yrityksen käyttämät verkkosivustot ovat ssl-suojattuja ja käyttävät https -yhteyttä pakotettuna. Yrityksen sisäverkkoon pääsee ulkopuolelta vain käyttäen suojattua vpn-yhteyttä. Tietoturvallisuus pidetään hyvällä tasolla ammattitaitoisen henkilökunnan toimesta.

6.5 Kehitysehdotukset

Rekisterinpitäjänä yrityksen pitää tehdä henkilötietojen käsittelijöiden kanssa sopimukset, joissa sovitaan henkilötietojen käsittelystä yksityiskohtaisesti. Yrityksen työntekijöiden osalta tämä tarkoittaa vaitiolovelvollisuuden liittämistä työsopimuksiin ja sisäisen käsittelyohjeen luomista. Yrityksen ulkopuolisille käsittelijöille on myös syytä luoda sopimuspohja, joka voidaan pienillä muutoksilla allekirjoittaa rekisterinpitäjän ja käsittelijän toimesta. Sopimuksilla varmistetaan, että käsittelijän poikettua sovitusta rekisterinpitäjä ei joudu vastuuseen. Sopimus on myös käsittelijän lupaus noudattaa tietosuoja-asetusta kokonaisuudessaan.

Järjestelmien tietoturvasta on huolehdittu hyvin ja huolehditaan myös tulevaisuudessa, mutta tietoturvadokumentaatio on rajoitettua. Tietoturvasta vastuussa olevat henkilöt ovat ammattitaitoisia ja tietävät mitä he tekevät, mutta ulkopuolisen tarkastajan on vaikea varmentaa tietoturvan taso ilman kattavaa dokumentaatiota. Tietoturvaa olisi mahdollista vahvistaa lisäämällä ulkoverkon ja datakeskuksen välille nykyaikainen palomuuri, joka estää tehokkaasti mahdollisia uhkia sekä tarjoaa laajan ja yksityiskohtaisen kuvan datakeskuksen verkkoliikenteestä tehokkaalla seurannalla.

Yrityksen tietosuojasta vastaavat henkilöt voivat luoda yrityksen tietosuojaorganisaation, joka vastaa säännöllisestä menettelystä, jolla tietosuoja pidetään mukana muun kehityksen kanssa. Tietosuojaorganisaatiolla pitäisi olla säännöllinen kokoontumisajankohta esimerkiksi neljännesvuosittain.

Tietoturvaloukkauksen 72 tunnin ilmoitusaika on lopulta hyvin lyhyt, joten ilmoittamiseen pitää varautua ennakkoon tai ilmoitus on auttamatta myöhässä. Tietoturvaloukkausten varalle pitää tehdä toimintasuunnitelma sekä ilmoituspohja. Toimintasuunnitelmassa määritetään tietoturva-aukon korjaustoimenpiteet ja miten jo vuotaneiden tietojen haittavaikutuksia heikennetään. Ilmoituspohjassa on oltava valmiiksi määritelty ilmoitettavat aiheet, jotta loukkausilmoitusta ei tarvitse luoda tyhjästä poikkeustilanteessa.

7 TIETOSUOJAVASTAAVA

Tietosuoja-asetus määrää rekisterinpitäjän nimittämään organisaatiolleen tietosuojavastaavan tietyillä ehdoilla. Tietosuojavastaava on nimettävä, jos kyseessä on julkishallinnon elin, rekisterinpitäjän tai käsittelijän ydintehtävät edellyttävät laajamittaista ja järjestelmällistä henkilötietojen käsittelyä tai käsittely kohdistuu erityisiin henkilötietoryhmiin. Tietosuojavastaavaa nimitettäessä on otettava huomioon nimitettävän ammattipätevyys sekä tietämys tietosuojalainsäädännöstä. Lisäksi nimitettävä henkilö voi kuulua organisaation henkilöstöön tai olla ulkopuolinen palvelusopimuksella toimiva tietosuojavastaava. Tietosuojavastaavan yhteystiedot on julkistettava ja ilmoitettava valvontaviranomaiselle. (Euroopan unioni 2017)

7.1 Tietosuojavastaavan asema

Tietosuojavastaava on otettava mukaan kaikkiin henkilötietoa koskeviin kysymyksiin ja hänelle on annettava resurssit, pääsy henkilötietoihin sekä mahdollisuus ylläpitää asiantuntemustaan. Tietosuojavastaavalle on annettava vapaat kädet tehtäviensä suorittamiseen eikä hän saa ottaa vastaan ohjeita työhönsä. Tämän lisäksi tietosuojavastaavaa ei saa erottaa tai rankaista työnsä hoitamisesta. Rekisteröityjen on pystyttävä ottamaan yhteyttä tietosuojavastaavaan henkilötietojensa käsittelyyn liittyen. Tietosuojavastaavalla voi olla myös muita työtehtäviä, jos ne eivät aiheuta eturistiriitoja, sekä häntä sitoo salassapitovelvollisuus. (Yleinen tietosuoja-asetus 2016, luku 4)

7.2 Tietosuojavastaavat tehtävät

Tietosuojavastaavan tehtävä on huolehtia, että organisaatio noudattaa tietosuoja-asetusta. Tämä onnistuu jakamalla tietoa ja neuvoja, kouluttamalla käsittelevää henkilöstöä ja tekemällä yhteistyötä valvontaviranomaisen kanssa. Näiden tehtävien hoitoon on oltava riittävästi resursseja sekä oikeuksia organisaation sisällä. Tietosuojavastaava myös huolehtii, että henkilötietojen käsittelyyn liittyvä dokumentaatio on riittävää ja ajankohtaista. (Yleinen tietosuoja-asetus 2016, luku 4)

7.3 Toimeksiantajan tietosuojavastaava

Tietosuoja-asetuksen vaatimuksien mukaisesti toimeksiantajan ei tarvitse nimittää tietosuojavastaavaa, mutta se on suositeltavaa siitä huolimatta suuren asiakaskunnan seurauksena. (Euroopan unioni 2017) Tietosuojavastaavan nimittäminen selventää vastuunjakoa organisaation sisällä ja varmistaa, että tietosuojasta pidetään huolta myös jatkossa. Kun tietosuojavastaava on nimitetty, pitää hänen yhteystiedot julkistaa ja ilmoittaa Suomen tietosuoja-asetuksen valvontaviranomaiselle. Tietosuojavastaavalle pitää luoda jokin kanava, jota käyttäen rekisteröidyt ja valvontaviranomainen voivat ottaa häneen yhteyttä.

8 LOPUKSI

Euroopan unionin asettama yleinen tietosuoja-asetus on medianäkyvyyden perusteella aiheuttanut lähes kaikissa organisaatioissa useita kysymyksiä, hämmennystä ja joissain määrin jopa paniikkia. Noin 100-sivuinen asetus on hyvin tulkinnanvarainen ja ennakkotapauksien puutteen takia sen soveltamisen laajuudesta sekä viranomaistulkinnoista ei ole varmuutta. Tietosuoja-asetuksen perimmäisenä tarkoituksena on tehdä henkilötietojen suojelusta perusoikeus sekä yhtenäistää ja virtaviivaistaa henkilötietojen käsittelyn vaatimuksia Euroopan unionin sisällä.

Suomessa henkilötietojen käsittely on yleisesti hyvällä tasolla ja suuri osa tietosuoja-asetuksen vaatimuksista on jo sisällytetty Suomen lakiin. Henkilötietojen käsittelyä ei ole siis syytä luoda kokonaan uudestaan, vain tarkistaa ja vahvistaa tarpeen mukaan. Suurin tietosuoja-asetuksen tuoma muutos on osoitusvelvollisuus, joka edellyttää organisaatioilta kattavaa dokumentaatiota, käsittelysopimuksia ja käsittelyn tarkempaa seurantaa. Rekisterinpitäjien on siis jatkossa pystyttävä osoittamaan, että henkilötietoja käsitellään turvallisesti.

Lähtöoletuksen mukaisesti toimeksiantajan Euronic Oy:n henkilötietojen käsittely on turvallista, läpinäkyvää ja tarkoituksenmukaista. Täydennettävää toimeksiantajalla on dokumentaatiossa, henkilöstön kirjallisessa ohjeistuksessa sekä käsittelyn seurannassa. Näitä tarvitaan osoittamaan, että tietosuoja-asetusta noudatetaan täysimääräisesti. Tärkeää on myös luoda tietosuojaorganisaatio, jonka vastuulla on huolehtia, että puutteet korjataan ja tietosuoja-asetusta noudatetaan myös tulevaisuudessa. Tietoturvan osalta toimeksiantajalla on riittävästi resursseja ja ammattitaitoa huolehtiakseen järjestelmien turvallisuudesta. Tietoturvan dokumentaatiota on silti syytä lisätä ja luoda menettely, jolla yrityksen tietoturvaa ylläpidetään ja tarkistetaan sisäisesti esimerkiksi vuosittain.

Tietosuoja-asetusta sovelletaan 25.5.2018 alkaen. Tämän jälkeen on syytä seurata tarkkaan, miten tietosuojaviranomaiset tulkitsevat ja tarkistavat organisaatioiden tietojenkäsittelyä. Lähitulevaisuudessa tietosuoja-asetuksesta tulee myös ennakkotapauksia, jotka selventävät asetuksen käytännön toteutusta. Voidaan olettaa, että tietosuoja-asetuksen tulkinnat ja käytännön toteutukset vakiintuvat vasta muutaman vuoden kuluttua, jonka aikana on suositeltavaa seurata ja kehittää organisaation omia käsittelytoimia. Tietosuoja-asetus muuttuu jatkuvasti uuden teknologian mukana ja organisaatioiden on oltava valppaana muuttumaan sen mukana.

LÄHTEET

Euroopan parlamentti ja neuvosto 2016. Yleinen tietosuoja-asetus. Bryssel. Viitattu 21.4.2018 http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Euroopan unioni. 2017. Tietosuoja. ISBN 978-92-79-65147-2.

Oikeusministeriö 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Helsinki. ISBN 978-952-259-558-4. Viitattu 21.4.2018 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimisto 2015. EU:n tietosuojauudistus. Viitattu 21.4.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. ISBN 978-952-251-778-4. Viitattu 21.4.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128