Juho Pärkkä

KOOSTEOPINNÄYTETYÖ: SYKKEEN MITTAAMINEN RANTEESTA JA EU:N UUTEEN TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN

KOOSTEOPINNÄYTETYÖ: SYKKEEN MITTAAMINEN RANTEESTA JA EU:N UUTEEN TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN

Juho Pärkkä
Opinnäytetyö
Kevät 2017
Tietotekniikan koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan koulutusohjelma, hyvinvointiteknologia

Tekijä: Juho Pärkkä
Opinnäytetyön nimi: Koosteopinnäytetyö: Sykkeen mittaaminen ranteesta ja EU:n uuteen tietosuoja-asetukseen valmistautuminen
Työn ohjaajat: Kaisa Orajärvi, Veijo Väisänen
Työn valmistumislukukausi ja -vuosi: Kevät 2017 Sivumäärä: 8 + 2 liitettä

Opinnäytetyö tehtiin kahdessa osassa. Ensimmäinen osa käsitteli sykkeen mittaamista ranteesta ja toinen osa EU:n uuden tietosuoja-asetuksen määrittämiä prosesseja tietomurrossa.

Ensimmäisen osan tavoitteena oli selvittää, mihin tekniikkaan sykkeen mittaaminen ranteesta perustuu, sekä mitä fysiologisia signaaleja käytetään. Työssä tutustuttiin myös sykettä mittaviin laitteisiin ja niiden valmistajiin.

Opinnäytetyön toisessa osassa tutkittiin, miten Mediracerin tulisi valmistautua uuteen EU:n tietosuoja-asetukseen sekä mitä asioita yrityksen tulee ottaa huomioon uuden asetuksen tullessa voimaan. Työssä selvitettiin myös, miten tulee toimia tietomurron sattuessa sekä miten uusi tietosuoja-asetus vaikuttaa pilvipalveluihin. EU:n yleinen tietosuoja-asetus hyväksyttiin keväällä 2016 ja sitä ryhdytään soveltamaan kahden vuoden siirtymäajan jälkeen keväällä 2018.

Asiasanat: sykkeen mittaus, tietosuoja, tietomurto, GDPR, pilvipalvelu

SISÄLLYS

1 JOHDANTO

Opinnäytetyö toteutettiin koosteopinnäytetyönä kahdessa osassa. Ensimmäinen osa oli laajuudeltaan 5 opintopistettä ja toinen osa 10 opintopistettä. Ensimmäisen osan teko oli jo keväällä 2015 ja toinen osa tehtiin keväällä 2017. Koosteessa työt esitellään lyhyesti ja varsinaiset osaopinnäytetyöt löytyvät liitteenä tämän koosteen lopusta.

2 ENSIMMÄISEN OSAN ESITTELY

Opinnäytetyön ensimmäisen osan (liite1) tarkoituksena oli perehtyä sykkeen mittaamiseen ranteesta. Työssä tutustuttiin, mihin tekniikkaan mittaaminen perustuu, sekä mitä fysiologisia signaaleja käytetään. Otettiin myös selvää, mitä laitteita sillä hetkellä oli markkinoilla ja ketä valmistajia.

Sykkeen mittaaminen aiheena liittyy keskeisesti hyvinvointiteknologia-alaan. Siinä yhdistyvät terveys ja teknologia. Opin tuntemaan ihmisen sydämen toimintaa paremmin ja erilaisia sykkeen mittausmenetelmiä. Pääpaino tässä työssä oli optisessa sykkeen mittaamisessa.

3 TOISEN OSAN ESITTELY

Toisen työn (liite 2) toimeksiantajana oli Mediracer Oy. Heillä tuli tarve perehtyä tietosuoja-asioihin uuden ohjelmistoprojektin sekä uuden EU:n tietosuoja-asetuksen myötä.

Työssä tutkittiin, miten EU:n uusi tietosuoja-asetus vaikuttaa yritykseen ja mitä yrityksen tulee ottaa huomioon uuden asetuksen tullessa voimaan. Asiaa lähestyttiin tietomurron näkökulmasta ja samalla selvitettiin myös muutoksia pilvipalveluihin.

Opinnäytetyön toinen osa ei liittynyt juurikaan suuntautumisvaihtoehtooni hyvinvointiteknologiaan, mutta tietotekniikkaan hyvin keskeisesti. Työssä käsiteltiin jonkin verran terveydentilaa koskevia tietoja eli potilastietoja, jotka kuuluvat olennaisesti hyvinvointiteknologiaan.

Ammatillisesti tämä työ opetti minua paljon. Tietosuoja ja tietoturva-asiat ovat todella tärkeitä aiheita kaikille, mutta erityisesti se koskee tietotekniikka-alaa. Opin työtä tehdessä tietosuoja-asioiden tärkeyden sekä lukemaan ja yksinkertaistamaan lakitekstejä.

4 YHTEENVETO

Opinnäytetyö koostui kahdesta erillisestä työstä. Ensimmäinen työ oli suuruudeltaan 5 opintopistettä ja liittyi sykkeen mittaamiseen ranteesta. Tämän työn aloitin jo keväällä 2015. Työ oli teoriapainotteinen ja aiheen sai valita itse. Ensimmäisessä osassa ei ollut toimeksiantajaa.

Toinen työ oli suuruudeltaan 10 opintopistettä. Työn toimeksiantajana oli Mediracer Oy. Työ oli selvitystyyppinen ja aihe mietittiin yhdessä Mediracerin sekä alihankkijayritys Haltianin kanssa.

Työn aiheiden eroavaisuus teki koosteen tekemisestä haasteellisen, mutta kokonaisuutena oli mielekästä toteuttaa työt erillisinä osina. Työmäärä jakaantui tasaisemmin koko opiskeluajalle.

Opinnäytetyö opetti minua kirjoittamaan isompia tekstikokonaisuuksia ja kehitti ammattitaitoa etenkin tietosuoja-asioissa huimasti. Uskon, että tämän työn jälkeen minulla on paremmat valmiudet työelämään.

LIITE 1

OULUN AMMATTIKORKEAKOULU

Juho Pärkkä

SYKKEEN MITTAAMINEN RANTEESTA

SYKKEEN MITTAAMINEN RANTEESTA

Juho Pärkkä
Opinnäytetyö, osa 1
Kevät 2015
Tietotekniikan koulutusohjelma
Oulun ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

Tämän insinöörityön tarkoituksena on tutkia sydämen sykkeen mittaamista ranteesta. Työssä selvitetään, mihin tekniikkaan mittaaminen perustuu, sekä mitä fysiologisia signaaleja käytetään. Lisäksi tutustutaan sykettä mittaaviin laitteisiin sekä niiden valmistajiin.

Sykemittareita on ollut olemassa jo pitkän aikaa. Lähiaikoina erilaiset hyvinvointirannekkeet ja rannetietokoneet ovat alkaneet yleistymään. Tässä opinnäytetyössä tutkitaan, millä eri tavoin syke saadaan ranteesta mitattua ja kuinka luotettavasti. Tämä on ensimmäinen osa kaksiosaista opinnäytetyötäni.

2 SYKE

Syke (syketaajuus) tarkoittaa sydämen lyöntitiheyttä. Se kertoo, kuinka tehokkaasti verenkiertoelimistö kuljettaa happea keuhkoista lihaksiin. Sydänlihas pystyy muodostamaan oman sähköisen signaalin ilman ulkopuolista ärsykettä. Sydänlihassyistä muodostuneessa impulssinjohtojärjestelmässä syntyy aktiopotentiaali, mistä se siirtyy sydämen eri osiin. Tässä järjestelmässä on sinussolmuke, eteisradat, eteis-kammiosolmuke ja eteis-kammiokimppu sekä siihen liittyvät haarat. Impulssi leviää johtojärjestelmästä tavallisiin sydänlihassoluihin, josta seuraa solujen supistuminen. (1, s.192–193.)

2.1 Sydämen toiminta

Sydän on verenkierron lihaspumppu, jonka tehtävänä on pumpata verta ruumiin eri osiin. Iso verenkierto pumppaa hapekasta verta elimistöön ja pieni verenkierto vähähappista verta keuhkoihin. Keuhkoissa veri hapettuu uudelleen. Ihminen tarvitsee happea elintoimintojensa ylläpitämiseen. Sydämen toimintakierrossa on kaksi säännöllistä vaihetta: supistumisvaihe eli systole ja veltostumisvaihe eli diastole. Diastolevaiheessa veri virtaa sydämeen ja systolevaiheessa sydän pumppaa verta verenkiertoon. Sydänlihaksen supistuksen saavat aikaan sydänlihassolut, joihin johtoratajärjestelmän solut johtavat aktiopotentiaaleja. (1, s. 186–200.)

2.2 Leposyke

Leposyke tarkoittaa lepotilassa saavutettua sykettä. Aikuisen ihmisen sydän lyö lepotilassa yleensä 60–80 kertaa minuutissa. Sydän reagoi ruumiillisiin ponnistuksiin sen mukaan, miten henkilö on tottunut niihin. Harjoittelemattoman huonokuntoisen henkilön leposyke voi olla esimerkiksi 90 bpm (beats per minute eli lyöntiä minuutissa). Tällaisen ihmisen sydän saavuttaa melko nopeasti maksimisykkeensä. (1, s. 186–200.)

Hyväkuntoisen harjoitelleen henkilön leposyke on usein hidas. Maratoonareilla leposyke voi olla jopa vain 35 bpm. Kun kaksi erikuntoista henkilöä on päässyt rasituksessa samaan suoritustasoon, on parempikuntoisen syke pienempi. Harjoitelleella on täten mahdollisuus vielä lisätä rasitusta, koska maksimisyke on kauempana. (1, s. 186–200.)

2.3 Maksimisyke

Ruumiillisen rasituksen aikana sydämen syketaajuus kasvaa eli syke nousee. Maksimisyke tarkoittaa syketaajuutta, jota nopeammin sydän ei pysty supistumaan. Tavallisen terveen nuoren henkilön maksimisyke on noin 200 bpm. Se pienenee iän myötä, ja esimerkiksi 60-vuotiaiden keskimääräinen maksimisyke on hieman yli 170. Taulukosta 1 nähdään normaalit tavoitesykealueet. Maksimisyke ei riipu treenauksesta, vaan harjoitellut henkilö vain saavuttaa sen hitaammin kuin harjoittelematon. Sykkeitä tarkasteltaessa on tärkeä muistaa, että yksilölliset vaihtelut ovat suuret. (1, s. 186–200.)

TAULUKKO 1. Tavoitesykealueet (2, s. 4)

% maksimisykkeestä	**Selite**
50-60%	Kevyt liikunta
60-70%	Kohtuullinen liikunta
70-80%	Aerobinen harjoittelu
80-90%	Anaerobinen harjoittelu

3 SYKKEEN MITTAUSMENETELMÄT

Sydämen syke on paras palaute kehon rasitustason mittaukseen liikunnan aika. Sykettä voi mitata monella eri tapaa. Sen voi mitata tunnustelemalla valtimoa ranteesta tai kaulalta ja laskemalla sydämen lyönnit. Tämä mittaustapa on kuitenkin vain suuntaa antava, joten tarkemman tuloksen saa sykemittarilla.

3.1 Sykemittari

Sykemittari koostuu rintakehälle asetettavasta lähettimestä ja lähettimen kiinnitysvyöstä sekä ranteessa pidettävästä vastaanottimesta. Se on laite, jonka avulla liikkuja saa välitöntä palautetta liikunnan rasittavuudesta. Mittaus perustuu samaan tekniikkaan kuin EKG-mittaus. Rinnalle asetettavaan lähetinvyöhön kiinnitetyt elektrodit välittävät sydänlihaksen sähköiset impulssit langattomasti ranteessa pidettävään vastaanottimeen. (3, s. 46.)

On todettu, että sykemittarit saattavat ottaa häiriöitä muista elektronisista laitteista. Häiriöt aiheuttavat yleensä tiedon häviämistä tai virheellistä dataa. Ongelmaa saattavat aiheuttaa myös eri sykemittareiden samat taajuusalueet. Lähellä olevat saman taajuiset sykemittarit saattavat sekoittaa tietoja keskenään. Tähän ratkaisuksi on kehitetty koodattu lähetin, joka toimii vain tietyissä mittareissa. (2, s. 14.)

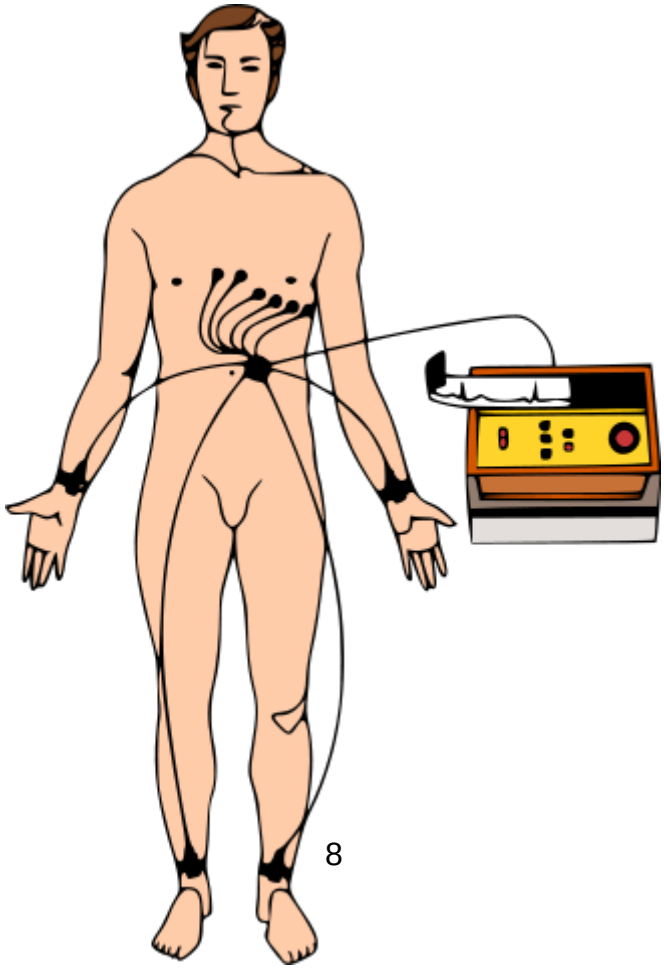
3.2 Palpaatiomittaus

Yksinkertaisimmillaan sykkeen voi mitata manuaalisesti laskemalla sydämen sykäysten lukumäärän minuutissa. Helpoiten pulssin tuntee, kun asettaa etu- ja keskisormen kevyesti ranteen peukalonpuoleiselle sisäsivulle valtimon päälle jänteiden viereen. Mittausta voi helpottaa vielä laskemalla pulssien määrä esimerkiksi 15 sekunnin ajan ja kertoa saatu luku neljällä. Näin saadaan lyöntien määrä minuutissa. (4.)

On tutkittu, että manuaalisesti mittaamalla virhe on sitä suurempi, mitä korkeampi syke on. Tavallisesti tunnustelemalla saadaan todellista sykettä alhaisempi lukema. Pitkän mittausajan takia syke ehtii myös laskea useita lyöntejä mittauksen aikana. Suuntaa antavana ja pulssin vaihteluun tutustuttaessa palpaatiomenetelmä on kuitenkin oivallinen ratkaisu. (4.)

3.3 Sykkeen mittaus EKG-mittarilla

Elektrokardiogrammi (EKG) eli sydänkäyrä kuvaa kahden elektrodin välisen jännitteen muuttumista ajan funktiona. EKG:n mittaaminen perustuu heikkojen sähköimpulssien mittaamiseen. EKG:ssä näkyvät sydänlihaksen depolarisaation aiheuttamat sähkövirran vaihtelut. Vertailukelpoisten tulosten saavuttamiseksi on kehitetty standardoitu mittausmenetelmä, jossa elektrodit asetetaan tietyille paikoille. Pintaelektrodit kiinnitetään joka raajaan, sekä kuusi elektrodia rintakehälle riviin rintalastan oikeasta laidasta vasempaan kupeeseen (kuva 1). EKG-mittauksella pystytään havaitsemaan helposti reaaliajassa sydämen toimintahäiriöt. (5.)



KUVA 1. Pintaelektrodien sijoittaminen (6)

4 SYKKEEN MITTAAMINEN RANTEESTA

Nykyiset sykemittarit edellyttävät sykevyön rinnan ympärille. Vaikka tähän vyöhön on aikaa myöten totuttu, ei se silti ole kovin mukava käyttää. Liikkeessä ja kovan hikoilun aikana sykevyö saattaa löystyä ja näin aiheuttaa tuloksissa epätarkkuuksia. Eri yritykset ovat huomanneet tämän ongelman ja alkaneet kehittää ranteeseen puettavia rannesykemittareita.

Rannesykemittarit mittaavat veren virtauksen optisesti. Virtausta tarkkaillaan valon eri aallonpituuksilla sekä valon eri voimakkuuksilla. Näiden avulla laite laskee sydämen sykkeen ja kertoo myös harjoittelun edistymisestä.

4.1 Optinen sykkeenmittaus

Valmistusmenetelmien tullessa halvemmiksi ja helpommiksi yritykset voivat tarjota kuluttajille samoja laitteita, jotka ovat aikaisemmin olleet vain ammattilaisten etuoikeus. Hyvinvointirannekkeissa käytettävät optiset sykesensorit käyttävät hyväkseen fotopletysmografiaa (PPG) sykesignaalin havaitsemiseen. PPG:tä on tavallisesti käytetty sairaaloissa happisaturaation määrittämiseen, mutta samalla tekniikalla on mahdollista mitata myös syketaajuus (kuva 2). Mittausmenetelmä perustuu valon aistimiseen. Valo lähetetään iholle ja se on yhteydessä kudokseen. Verisuonten koostumus vaihtuu samanaikaisesti sydämen sykkeen kanssa ja täten vaihtuu myös sitten valon voimakkuus. (7, s. 3.)

KUVA 2. Adidas miCoach Smart Run -älykello (8)

4.2 Fotopletysmografia (PPG)

Fotopletysmografia on yksinkertainen ja halpa kudosten pintaverenkierron tutkimusmenetelmä. Menetelmä on noninvasiivinen, eli siinä ei läpäistä ihoa millään instrumentilla. Se perustuu veren punasolujen kykyyn imeä kudosta läpäisevää infrapunasäteilyä. Tällä menetelmällä voidaan tutkia muun muassa virtaavan veren kokonaistilavuutta, sykepulssia sekä veressä olevan hapen määrää. (9.)

5 LAITTEITA JA VALMISTAJIA

Terveys ja fitness ovat tämän ajan trendejä. Sen ovat huomanneet monet hyvinvointiteknologia-alan yrityksetkin. Ihmisiä kiinnostavat oma keho ja sen käyttäytyminen. Viime vuosina älypuhelinten myötä ovat yleistyneet erilaiset askelmittari- ja kuntoilusovellukset. Nämä sovellukset eivät kuitenkaan pysty tarjoamaan sykkeenmittausta.

Fotopletysmografian avulla sykkeenmittaus onnistuu pienellä rannelaitteellakin. Ei tarvita kuin yksi LED, joka lähettää valoa, ja yksi anturi, joka vastaanottaa valoa. Loput toiminnot hoitaa rannelaitteessa sijaitseva laskentayksikkö.

5.1 PulseOn

PulseOn on suomalainen hyvinvointiteknologia-alan yritys, joka valmistaa PulseOn-sykemittaria. Se on perustettu vuonna 2012, ja päätoimipaikka sijaitsee Espoossa. Yritys työllistää 14 työntekijää. PulseOnin toimitusjohtaja on Tero Mennander. PulseOn on entisten Nokian insinöörien ja asiantuntijoiden perustama kasvuyhtiö. (10.)

PulseOn-rannelaitteen pohjassa on kolme LED-valoa sekä valoa aistiva sensori. Sensori näkee verisuonissa virtaavan veren liikkeen. PulseOn-rannelaitteessa ei siis ole erillistä sykevyötä (kuva 3). Laite kertoo myös muuta tietoa kuin sykkeen. Se analysoi harjoitteen vaikutusta ja laskee kulutettuja kaloreita. Algoritmit kalorien laskentaan tekee Firstbeat niminen yritys Jyväskylästä. (10.)

KUVA 3. PulseOn-rannelaite (vasemmalla) ja mobiilisovelluksen kuvakaappaus (oikealla) (11)

5.2 Mio Global

Mio Global syntyi, kun Liz Dickinson halusi helpon tavan seurata harjoitussuunnitelmaa sekä kalorimäärää. Hän halusi huolettoman sykemittarin ilman vyötä. Teknologian tähän hän löysi Hollannista Philips Electronicsilta. Mio Globalin optiset laitteet käyttävät kahta vihreää LED-valoa sykkeen mittaamiseen (kuva 4). (7, s. 23–24.)

Mio Globalin ensimmäinen laite oli Mio Alpha (kuva 4). Siinä oli patentoitu kalorihallintajärjestelmä yhdessä optisen sykkeenmittauksen kanssa. Laite oli mahdollista kytkeä erilaisiin sovelluksiin ja muihin laitteisiin Bluetooth-yhteyden kautta. (7, s. 23–24.)

KUVA 4. Mio Alpha -rannesykemittari (12)

Viime aikoina Mio Global on tehnyt yhteistyötä muiden yritysten kanssa saadakseen rannesykemittarit laajemman yleisön tietoisuuteen. Muun muassa TomTom ja Adidas ovat integroineet Mio-teknologiaa uusimpiin älykelloihinsa. (7, s. 23–24.)

6 YHTEENVETO

Työn tarkoituksena oli tutkia sydämen sykkeen mittaamista ranteesta. Työssä selvitettiin, mihin tekniikkaan mittaaminen perustuu sekä mitä fysiologisia signaaleja käytetään. Tutustuttiin myös eri rannesykemittareihin sekä niiden valmistajiin.

Uskon, että tulevaisuudessa rannesykemittarit ja älykellot tulevat yleistymään entisestään. Tähän vaikuttavat hintojen tippuminen sekä tuotteiden näkyvyyden paraneminen. Nähtäväksi jää, kuinka suuren suosion ne lopulta saavuttavat.

Mielestäni tavoitteisiin päästiin. Opin paljon sydämen sykkeestä, sen mittaamisesta, sekä erityisesti optisesta sykkeen mittaamisesta, mikä olikin tämän insinöörityön ensimmäisen osan pääaihe. Mielenkiinto aihetta kohtaan kasvoi työn edetessä ja toivon, että tulen jatkossakin työskentelemään aiheen parissa.

LÄHTEET

1. Nienstedt, Walter − Hänninen, Osmo − Arstila, Antti − Björkqvist, Stig-Eeyrik 1995. Ihmisen fysiologia ja anatomia 10. painos. Porvoo: WSOY, S. 186– 200.

2. Aro, Olli – Gustafsson, Esa – Karjalainen, Petri 2011. Tekstiilipannan luotettavuuden ja käytettävyyden arviointi 24 tunnin sykevälimittauksessa. Saatavissa: http://www.firstbeat.com/userData/firstbeat/tiedostolatauk-set/Aro_Gustafsson_Karjalainen_2011.pdf. Hakupäivä 10.4.2015.

3. Edwards, Sally 1993. Sykettä elämään. Suom. Raija Laukkanen. Kempele: Polar Electro Oy.

4. Sykkeenmittaus. 2014. Edu.fi. Saatavissa: http://www.edu.fi/perusopetus/liikunta/teknologia_liikunnanopetuk-sessa/sykkeenmittaus. Hakupäivä 27.3.2015.

5. Romppainen, Matti 2010. Elektrokardiografia (EKG). Saatavissa: http://users.jyu.fi/~peltsi/ali/opetus/hyvotek/LBIA020_raportit.htm. Hakupäivä 10.4.2015.

6. Madhero88. 2009. Potilas sydänsähkökäyrässä. Saatavissa: http://fi.wi-kipedia.org/wiki/Sydänsähkökäyrä#/media/File:ECGcolor.svg. Hakupäivä 21.4.2015.

7. Haavikko, Aleksi 2014. Evaluation of performance of an optical heart rate sensor. Saatavissa: https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/22628/haa-vikko.pdf?sequence=1&isAllowed=y. Hakupäivä 27.3.2015.

8. Adidas miCoach Smart Run: älyä ranteessa. 2014. Läskimaija. Saatavissa: http://laskimaija.blogspot.fi/2014/03/adidas-micoach-smart-run-alya-ranteessa.html. Hakupäivä 12.5.2015.

9. Laapotti, Pekka 2009. Fotopletysmografia verenkierron tutkimusmenetelmänä. Saatavissa: http://batman.jamk.fi/~voyager/opin/index.php?nayta=7436. Hakupäivä 27.3.2015.

10. Mäntylä, Juha-Matti 2014. Minä mittarissa. Saatavissa: http://lehtiarkisto.talentum.com/lehtiarkisto/search/show?eid=2738290. Hakupäivä 17.4.2015.

11. PulseOn color cloud. 2014. PulseOn. Saatavissa: http://euro.pulseon.com/pulseon-color-cloud.html. Hakupäivä 17.4.2015.

12. Mio Alpha Heart Monitor Sports. 2015. Amazon.com. Saatavissa: http://www.amazon.com/Mio-Alpha-Heart-Monitor-Sports/dp/B00DEQ7WVM. Hakupäivä 21.4.2015.

LIITE 2

OULUN AMMATTIKORKEAKOULU

Juho Pärkkä

EU:N UUDEN TIETOSUOJA-ASETUKSEN MÄÄRITTÄMÄT PROSESSIT TIETOMURROSSA

EU:N UUDEN TIETOSUOJA-ASETUKSEN MÄÄRITTÄMÄT PROSESSIT TIETOMURROSSA

Juho Pärkkä
Opinnäytetyö, osa 2
Kevät 2017
Tietotekniikan koulutusohjelma
Oulun ammattikorkeakoulu

SISÄLLYS

LYHENTEET

DPIA	Data Protection Impact Assessment. Vaikutustenarviointi.
ETA	Euroopan talousalue
EU	Euroopan unioni
GDPR	General Data Protection Regulation. EU:n tietosuoja-asetus.
PoC	Point of Care. Hoitopaikkatesti.
PDCA	Plan, Do, Check, Act. Suunnittele, toteuta, arvioi, toimi.

1 JOHDANTO

Nykypäivänä tietosuoja ja tietoturva-asiat ovat tärkeässä roolissa. Ihmisistä kerätään jatkuvasti dataa eri käyttötarkoituksiin. On hyvä, että lainsäädäntö antaa raamit, mikä on oikea ja laillinen tapa kerätä tietoa.

Opinnäytetyö on jaettu kahteen osaan ja tämä on opinnäytetyön toinen osuus. Ensimmäinen työ liittyi sykkeen mittaamiseen ranteesta ja se oli 5:n opintopisteen laajuinen. Tämä toinen osa on laajuudeltaan 10 opintopistettä. Tilaajana tässä työssä toimii Mediracer Oy. Mediracerilla tuli tarve perehtyä tietosuoja-asioihin uuden ohjelmistoprojektin sekä uuden EU:n tietosuoja-asetuksen myötä. Yrityksen, jonka ydinliiketoiminta on tarjota lääketieteeseen liittyviä palveluja ja sitä kautta tallentaa potilastietoja, on tärkeää hallita tietosuoja-asiat.

Opinnäytetyössä tutkitaan, miten Mediracerin tulisi valmistautua uuteen EU:n tietosuoja-asetukseen prosessien kannalta sekä mitä asioita yrityksen tulee ottaa huomioon uuden asetuksen tullessa voimaan. Työssä selvitetään, miten tulee toimia tietomurron sattuessa. Mietitään muun muassa, kenelle täytyy raportoida, minkä ajan sisällä ja millaiset ovat sanktiot. Opinnäytetyössä selvitetään myös, miten uusi tietosuoja-asetus vaikuttaa pilvipalveluihin. EU:n yleinen tietosuoja-asetus hyväksyttiin keväällä 2016 ja sitä ryhdytään soveltamaan kahden vuoden siirtymäajan jälkeen keväällä 2018.

2 TIETOSUOJA

Tietosuoja on yksityisyyttä suojaava perusoikeus. Siihen kuuluu kansalaisten yksityisyyden suojan ja oikeusturvan huomioiminen muun muassa tietojen rekisteröinnissä ja tiedostojen suojaamisessa luvattomalta ulkopuoliselta käytöltä (1, s. 15.)

Tietosuojassa on kyse asiakkaan luottamuksesta ja asiakastietojen asiallisesta ja oikeaoppisesta käsittelystä tiedon elinkaaren eri vaiheissa. Tietosuojaosaamisen puutteesta voi seurata tehottomuutta, mistä johtuu, ettei saavuteta kustannussäästöjä. Potilasturvallisuus, työntekijöiden oikeusturva sekä yksityisyyden suoja voivat vaarantua. Kun organisaatio huolehtii tietosuojasta, se näyttäytyy ulospäin luotettavana ja houkuttelevana yhteistyökumppanina. (2, s. 4.)

2.1 Tietosuojan ja tietoturvan käsitteitä

Tietosuojalla tarkoitetaan yksilön yksityisyyden ja luottamuksen turvaamista, kuten henkilötietojen oikeaoppista käsittelyä sekä niiden suojaamista luvattomalta käytöltä ja muulta käsittelyltä. Henkilön oikeus saada tietää itseään koskevista henkilörekisteritiedoista kuuluu myös tietosuojaan. (3.)

Tietoturvan tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus niin, ettei niiden luottamuksellisuus, eheys ja saatavuus kärsi. Kuvassa 1 on kiteytettynä tietosuojan toteutuminen. (3.)

KUVA 5. Tietosuojan toteutuminen (4, s. 8)

Tietosuojassa on kyse rekisteröidyn oikeuksista. Tietoturvalla taas tarkoitetaan niitä keinoja, teknisiä ja hallinnollisia toimenpiteitä, joilla edellä mainitut rekisteröidyn oikeudet turvataan. (3.)

2.2 Tietomurto

Tietomurto tarkoittaa tunkeutumista suojattuun tietojärjestelmään tai tietoverkkoon. Tietoturvaloukkaus tarkoittaa oikeudetonta puuttumista tietoturvaan. Tietomurto on rangaistava teko ja se on kirjoitettu rikoslakiin seuraavasti. (5, s. 14–16.)

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen

> avulla tai muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta. (6.)

Tietomurto on törkeä, jos se on järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallinen ja kokonaisuutena arvostellen törkeä. Rikoksentekijä on tuomittava tällöin sakkoon tai vankeuteen enintään kolmeksi vuodeksi. Molemmissa tapauksissa, tietomurrossa sekä törkeässä tietomurrossa, pelkkä yrityskin on rangaistavaa. (6.)

2.3 Tietosuojaan liittyvät roolit, oikeudet ja velvollisuudet

EU:n tietosuoja-asetuksessa käsiteltävät roolit voidaan jakaa neljään osaan, joilla jokaisella on omat velvollisuutensa ja oikeutensa. Roolit ovat rekisterinpitäjä, henkilötietojen käsittelijä, rekisteröity ja valvontaviranomainen (kuva 2). (7, s. 4.)

KUVA 6. Tietosuojaan liittyvät roolit (7, s. 6)

2.3.1 Rekisterinpitäjä

Rekisterinpitäjä on luonnollinen henkilö, viranomainen, oikeushenkilö, virasto tai muu elin, joka yksin tai yhdessä toisten tahojen kanssa määrittää henkilötietojen käsittelyn keinot ja tarkoitukset. Yleensä rekisterinpitäjän rooli perustuu organisaation toiminnalliseen suhteeseen yksilön kanssa. Esimerkki rekisterinpitäjästä voisi olla yritys, joka myyntitoiminnassaan käsittelee asiakastietoja tai työnantaja, joka käsittelee työntekijöidensä työsuhteeseen liittyviä tietoja. Rekisterinpitäjän rooli voi myös perustua lainsäädännöllisiin tai organisaation virallisiin tehtäviin. Esimerkiksi kansalaisten verotukseen liittyville taloudellisille tiedoille rekisterinpitäjä on veroviranomainen. Rekisterinpitäjän rooli voi perustua organisaation tosiasialliseen määräysvaltaan tietojenkäsittelyssä. Tämä koskee lähinnä konserneja, joissa emoyhtiöllä on määräysvalta tytäryhtiöön. Esimerkki tällaisesta voisi olla, että organisaation pääkonttori vaatii tytäryhtiötä käyttämään tiettyä pilvisovellusta. Toinen esimerkki liittyen tosiasialliseen määräysvaltaan on, että varastettujen henkilötietojen rekisterinpitäjäksi katsotaan henkilötiedot varastanut taho. Taholla ei ole riittävää oikeusperustaa henkilötietojen käsittelyyn, mikä tekee siitä laitonta. (7, s. 4.)

Rekisterinpitäjä on vastuussa henkilötietojen käsittelystä ja vastaa mahdollisista tietosuoja-asetuksen rikkomiseen liittyvistä vahingoista. Jos rekisterinpitäjä käsittelee henkilötietoja yhdessä toisen rekisterinpitäjän kanssa, kukin rekisterinpitäjä on yhteisvastuullisesti vastuussa rekisteröidyille. (7, s. 5.)

2.3.2 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun. Käsittelijänä voi olla esimerkiksi tietotekniikan palveluntarjoaja tai palkkahallinnon ammattilainen. Henkilötietojen käsittelijä ei saa käyttää henkilötietoja omiin tarkoituksiinsa, vaan hänen on käsiteltävä tietoja rekisterinpitäjän ohjeiden mukaisesti. (7, s. 5.)

Henkilötietojen käsittelijän on käsiteltävä henkilötietoja sisäänrakennetun tietosuojan ja oletusarvoisen tietosuojan mukaisesti. Henkilötietojen käsittelijä on

vastuussa omien velvollisuuksiensa laiminlyönneistä, mutta on myös syytä huomioida, että rekisterinpitäjällä on aina oma vastuunsa. Siksi onkin tärkeää, että heidän välillään on sopimus, jossa sovitaan kummankin osapuolen velvollisuuksista. (7, s. 5.)

2.3.3 Rekisteröity

Rekisteröity tarkoittaa henkilöä, jota henkilötieto koskee. Uusi tietosuoja-asetus antaa rekisteröidyille uusia erityisoikeuksia (kuva 3). Esimerkiksi rekisteröidyillä on oikeus saada ilmoitus tietojenkäsittelystä, oikeus antaa suostumus tai vastustaa omien henkilötietojen käsittelyä. Rekisteröidyillä on myös oikeus siirtää tiedot järjestelmästä toiseen, oikeus olla joutumatta automaattisen tietojenkäsittelyn tai profiloinnin kohteeksi, oikeus tulla unohdetuksi sekä oikeus tehdä valitus valvontaviranomaiselle ja saada vahingonkorvausta, jos rekisterinpitäjä tai henkilötietojen käsittelijä on laiminlyönyt tehtäviään. (7, s. 5.)

KUVA 3. Rekisteröidyn oikeudet (4, s. 7)

2.3.4 Valvontaviranomainen

Valvontaviranomainen eli tietosuojaviranomainen on kansallinen viranomainen, joka valvoo tietosuoja-asetuksen täytäntöönpanoa jäsenvaltioiden alueella. Valvontaviranomaisten tehtäviin kuuluu muun muassa langettaa sakkoja, suorittaa

tutkimuksia ja käsitellä valituksia. Rekisterinpitäjät ilmoittavat tietosuojaviranomaiselle mahdollisista tietoturvaloukkauksista. Jotkin tietojenkäsittelytoimet, kuten kansainväliset tiedonsiirrot, saattavat edellyttää tietosuojaviranomaisten lupaa. (7, s. 6.)

3 EU:N UUDEN TIETOSUOJA-ASETUKSEN MUUTOKSET JA VALMISTAUTUMINEN

Euroopan unionin yleinen tietosuoja-asetus hyväksyttiin huhtikuussa 2016 ja sitä aletaan soveltaa kahden vuoden siirtymäajalla toukokuussa 2018. Uuden tietosuoja-asetuksen päätavoitteena on suojella kansalaisten henkilötietoja, lisätä organisaatioiden vastuita ja velvollisuuksia sekä yksinkertaistaa ja yhdenmukaistaa sääntelyjä. Asetus on vahvin määräys, jonka Euroopan unioni voi antaa. Direktiivi on ohje, jonka mukaan jäsenmaat laativat omat lakinsa. Jokainen valtio saa itse päättää, miten se toteuttaa direktiivin määräykset. Tultuaan voimaan asetus menee kaikkien kansallisten tietosuojalakien edelle, vaikka kansalliset säännökset olisivat tiukemmat. (7, s. 2.)

Tietosuoja-asetuksen muutoksella Euroopan unioni vastaa teknologian nopeaan kehitykseen ja digitalisaatioon. Uudistumisessa tulee lisää oikeuksia ja velvollisuuksia rekisterinpitäjille ja henkilötietoja käsitteleville tahoille. EU:n uusi tietosuoja-asetus tulee koskemaan kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa. Tavoitteena on yhdistää ja yhdenmukaistaa eurooppalaista tietosuojakäytäntöä. Tähän mennessä se on muodostunut jäsenvaltioiden omista epäyhtenäisistä toimintamalleista. Asetus velvoittaa EU:n ulkopuolisia toimijoitakin noudattamaan samoja säädöksiä tarjotessaan tuotteita tai palveluita EU:n kansalaisille. Kuvassa 4 on tiivistettynä asetuksen sisältö ja tavoite. (8.)

KUVA 4. Tietosuoja-asetuksen sisältö ja tavoite pähkinänkuoressa (2, s. 17)

3.1 Rekisteröidyn oikeudet

Henkilöä, jonka henkilötiedot on tallennettu rekisteriin, kutsutaan rekisteröidyksi. Rekisteröityjen oikeuksien pääperiaatteena on henkilötietojen suojan takaaminen valtuudettomalta ja henkilöä vahingoittavalta tietojen käytöltä. Uuden tietosuoja-asetuksen määrittelemät rekisteröityjen oikeudet ovat osin vastaavia kuin Suomen henkilötietolaissakin, mutta uuden asetuksen myötä rekisteröidyille tulee uusia oikeuksia vastaamaan teknologian ja henkilötietoja käsittelevien palveluiden kehitystä. (9.)

3.1.1 Henkilötiedot

Henkilötiedoilla tarkoitetaan kaikkia yksilöä koskevia tietoja, niin yksityistä kuin ammatillista ja julkistakin elämää koskevia tietoja. Henkilötietoihin kuuluvat muun muassa nimi, sähköpostiosoite, valokuva, pankkitiedot, terveydentilaa koskevat tiedot, ostokset, sijainti, käyttäjätunnus ja salasana sekä tietokoneen

IP-osoite. Tietosuoja-asetusta sovelletaan, kun henkilö voidaan tunnistaa tiedoista suoraan tai epäsuorasti tai kun henkilö voidaan tunnistaa ryhmästä henkilötietojen perusteella. (7, s. 3.)

Tällä hetkelläkin nykyisen henkilötietolain mukaan rekisteröidyllä on tiettyjä oikeuksia, muun muassa omien tietojen tarkistus, niiden oikaisu sekä poistaminen. Nämä vanhat oikeudet säilyvät, mutta uuden asetuksen myötä rekisteröity saa entistä vahvemman kontrollin omiin tietoihinsa. Uuden tietosuoja-asetuksen myötä yrityksen tulee antaa rekisteröidyille yhä enemmän, läpinäkyvämmin ja selkeämmin tietoa heidän tietojensa käsittelystä. (10.)

3.1.2 Arkaluonteiset tiedot

Arkaluonteisilla tiedoilla tarkoitetaan tietosuoja-asetuksessa henkilötietojen erityisiä tietoryhmiä. Ne voivat olla esimerkiksi sellaisia tietoja, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, geneettisiä tietoja, terveyttä koskevia tietoja tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Näitä arkaluonteisia tietoja koskeva käsittely on erikseen säänneltyä. (4, s. 10.)

Tietosuoja-asetuksessa korostetaan useaan otteeseen lasten henkilötietojen suojelemisen tärkeyttä. Huolellisuusvelvollisuus voidaan liittää myös muihin haavoittuvassa asemassa oleviin henkilöryhmiin, kuten ikääntyneisiin. Arkaluontoiseksi tiedoiksi katsotaan myös tietojenkäsittely, joka aiheuttaa suuria riskejä yksilöiden oikeuksille ja vapauksille. (7, s. 3.)

3.1.3 Profilointi

Rekisteröidyille tulee uuden asetuksen myötä myös uusia oikeuksia, kuten oikeus tietojen siirrettävyyteen sekä profiloinnista kieltäytymiseen. Profilointi on toimintaa, jossa asiakkaista kerättävien tietojen perusteella luodaan erilaisia kohderyhmiä ja luokitteluja. Tietojen siirrettävyys tarkoittaa tietojen siirtämistä ilman välikäsiä rekisterinpitäjien välillä. Profiloinnista kieltäytyminen taas tarkoittaa sitä, että rekisteröidyillä on oikeus kieltäytyä olemasta sellaisten päätösten

kohteena, jotka perustuvat automaattisella tietojenkäsittelyllä tapahtuvaan tiettyjen henkilökohtaisten ominaisuuksien arviointiin. Automaattinen tietojenkäsittely tarkoittaa sellaista tilannetta, jossa ihminen ei puutu asiaan mitenkään. Esimerkki profiloinnista voisi olla sähköisen rekrytoinnin käyttö ilman ihmisen osallistumista. (10.)

3.1.4 Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus poistattaa omat henkilötiedot, jos tietojenkäsittely ei ole enää tarpeellista tai sillä ei ole laillisia perusteita. Lisäksi rekisteröidyllä on oikeus saada omat henkilötiedot rekisterinpitäjältä yleisesti käytetyssä sähköisessä ja jäsennellyssä muodossa, jotta hänellä on mahdollisuus siirtää tiedot toiselle rekisterinpitäjälle. Tällä hetkelläkin rekisteröidyillä on oikeus pyytää ja saada itseään koskevat tiedot rekisterinpitäjältä, mutta formaattia, missä muodossa tietojen on oltava, ei ole määritelty. Tiedot voi siis saada tällä hetkellä vaikka paperisena. (8.)

3.2 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjän yksi päävelvollisuus on rekisteröidyn oikeuksien toteuttaminen. Tämän lisäksi uutena velvollisuutena asetus määrittelee muun muassa ilmoitusvelvollisuuden. Uusia viestittäviä asioita ovat henkilötietojen säilytysajat ja tietosuojavastaavan yhteystietojen ilmoittaminen. Rekisterinpitäjän tulee ilmoittaa rekisteröidyille asiat helposti ymmärrettävässä muodossa, ennen kuin henkilötietoja kerätään. Rekisterinpitäjän antama kuvaus henkilötietojen käsittelystä tulee pitää julkisesti saatavilla ja ajantasaisena. On erittäin suotavaa panostaa avoimeen ja läpinäkyvään viestintään käsittelytoimista ja rekisteröityjen oikeuksien toteutuksesta. (9.)

3.2.1 Tietosuojavastaava

Uuden tietosuoja-asetuksen myötä on suositeltavaa nimittää yrityksestä joku henkilö tietosuojavastaavaksi. Tietyissä tilanteissa se on jopa pakollistakin, ku-

ten julkisella sektorilla ja sellaisissa yrityksissä, joiden keskeiset tehtävät käsittelevät rekisteröityjen laajamittaista ja järjestelmällistä seurantaa tai laajamittaista arkaluonteisten tietojen käsittelyä. Tässä vaiheessa on vielä hieman tulkinnanvaraista, mitä laajamittainen seuranta tarkoittaa. Tietosuoja-asetuksessa itsessään ei kerrota tarkkaa määrä. Jos yrityksen ydintehtävät liittyvät terveydenhoitoalaan, tulee 37 artiklan 1 kohdan c-osasta vaatimus nimittää tietosuojavastaava. (10; 11, s. 55; 12.)

Tietosuojavastaavan rooli on yrityksessä itsenäinen ja hän raportoi suoraan korkeimmalle johdolle. Hänen tehtäviinsä kuuluu myös muun muassa henkilöstön kouluttaminen ja ohjeistus sekä yhteyshenkilönä toimiminen niin viranomaisten kuin rekisteröityjenkin kanssa. Jos kyseessä on konserni, riittää yksi tietosuojavastaava edellyttäen, että häneen voi ottaa helposti yhteyttä jokaisesta toimipaikasta (10; 11, s. 55.)

3.2.2 Ulkoinen palveluntarjoaja

Uusi tietosuoja-asetus edellyttää kirjallisen sopimuksen tekemistä ulkoisen palveluntarjoajan kanssa, joka käsittelee henkilötietoja, kuten pilvipalveluiden tarjoaja. Asetus asettaa tietyt sisällölliset vaatimukset sopimukselle. Jos yrityksellä on ulkoinen palveluntarjoaja, on hyvä käydä tämä sopimus läpi, että se vastaa myös jatkossa uuden asetuksen vaatimuksia. (10.)

3.2.3 Tilivelvollisuus

Yksi iso uudistus asetuksessa on tilivelvollisuus. Tämä vaatii rekisterinpitäjältä varautumista, kykyä todistaa toimenpiteet sekä riskilähtöistä ja ennakoivaa tietosuojan suunnittelua. Rekisterinpitäjän tai henkilötietojen käsittelijän on itse arvioitava käsittelyyn liittyvät riskit ja toteutettava toimenpiteitä näiden riskien lieventämiseksi. Käytännössä tämä tarkoittaa sitä, että tiedon käsittelijän pitää itse pystyä määrittelemään, miten tietoa suojataan, ja tarvittaessa osoittamaan se. Tämä on suhteellisen iso muutos vanhaan, sillä tällä hetkellä tietosuojaviranomainen on vastuussa siitä, että lainsäädäntöä noudatetaan. (8.)

3.2.4 Sakko

Asetusta rikkovalle voidaan langettaa hallinnollinen sakko, joka voi olla jopa 20 000 000 euroa tai 4 prosenttia yrityksen kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Jos kyseessä on vähäinen rikkomus tai kohtuuton rasitus henkilölle, voidaan sakon sijasta antaa myös huomautus. Jokaisella valvontaviranomaisella on valtuudet määrätä hallinnollisia sakkoja. Määrättävien sakkojen täytyy olla tehokkaita, oikeasuhtaisia ja varoittavia. (11, s. 82–83.)

3.2.5 Vastuu

Rekisterinpitäjä on vastuussa siitä, että henkilötietoja käsitellään asianmukaisesti ja laillisesti. Jos rekisteröidylle aiheutuu aineellista tai aineetonta vahinkoa, hänellä on oikeus saada korvaus rekisterinpitäjältä tai henkilötietojen käsittelijältä aiheutuneesta vahingosta. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta. (11, s. 81.)

Henkilötietojen käsittelijä on vastuussa vahingosta vain siinä tapauksessa, jos se ei ole noudattanut sille osoitettuja asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän ohjeistuksen ulkopuolella tai sen vastaisesti. Henkilötietojen käsittelijä sekä rekisterinpitäjä voidaan vapauttaa vastuusta, jos he pystyvät osoittamaan osallistumattomuutensa vahinkoon. (11, s. 81.)

3.2.6 Dokumentaatio

Rekisterinpitäjän tulee huolehtia asianmukaisesta tietosuojadokumentaatiosta liittyen osoitusvelvollisuuteen. Ajantasainen dokumentaatio on hyvä keino osoittaa valvontaviranomaiselle, että tietosuojasta huolehditaan asianmukaisella tavalla. On tärkeää huomata, että asiat pitää suhteuttaa organisaation kokoon ja henkilötietojen käsittelytarpeen määrään. Dokumentissa olisi hyvä olla seuraavat asiat: (4, s. 27–28.)

- Tietosuojapolitiikka
- Tietosuojaorganisaatio, sen roolit ja vastuut

- Tietosuojaselosteet
- Rekisterien tietovirta- ja vuokuvaukset
- Kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyistä prosesseista
- Tehdyt tietosuojan riski- ja vaikutustenarvioinnit hallintakeinoineen
- Tietosuojaa ja tietoturvaa käsittelevien foorumeiden ja ohjausryhmien pöytäkirjat
- Riskirekisterit ja kirjanpito riskien hyväksymisestä ja omistajuudesta.
- Tietoturvatestauksen tulokset
- Kuvaukset prosesseista, joilla taataan sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen
- Henkilötietoja käsitteleville henkilöstölle suunnattavat ohjeet
- Dokumentaatio mahdollisista henkilötietojen käsittelyssä tapahtuneista loukkauksista
- Tietotilinpäätös (keinona toteuttaa osoitusvelvollisuus) (4, s. 28.)

4 TIETOSUOJA JA PILVIPALVELUT

EU:n uutta tietosuoja-asetusta tulee noudattaa riippumatta siitä, millä tavoin henkilötietoja käsitellään. Asetus koskee yhtä lailla paikalliselle palvelimelle tallennettuja kuin pilvipalvelimelle tallennettuja henkilötietoja. Pilvipalvelut asettavat kuitenkin haasteita asetuksen noudattamiseen niille organisaatioille, jotka kuuluvat tietosuoja-asetuksen piiriin. (7, s. 6.)

Rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee tietää, missä paikassa henkilötietoja säilytetään ja käsitellään. Tietosuoja-asetus rajoittaa ankarasti mahdollisuutta siirtää henkilötietoja ETA:n eli Euroopan talousalueen ulkopuolelle. ETA:aan kuuluvat EU:n jäsenvaltioiden lisäksi Norja, Islanti ja Liechtenstein. Pilvipalvelut voivat käyttää ETA:n ulkopuolella sijaitsevia palvelimia tai Euroopan alueella sijaitseva pilvipalvelu voi olla ETA:n ulkopuolisen palveluntarjoajan hallinnassa. Näissä tapauksissa henkilötietojen siirron on tapahduttava tietosuoja-asetusten mukaisesti. (7, s. 6.)

Rekisterinpitäjien on toteutettava riittävät turvatoimet, jotta he pystyvät suojaamaan henkilötietojen häviämiset, muuttumiset ja luvattomat käsittelyt. Rekisterinpitäjän on myös arvioitava, täyttävätkö henkilötietojen käsittelijän tietoturvatoimet tietoturvavaatimukset henkilötietojen ja rekisterinpitäjän osalta. Tietoturvatoimien täytäntöönpanoa valvotaan suorittamalla säännöllisiä tarkastuksia. Samat vaatimukset koskevat myös alihankkijoita, jos henkilötietojen käsittely teetetään heillä. Pilvipalvelujen tarjoajat eivät kuitenkaan välttämättä salli asiakkaiden antaa tietoturvaa koskevia ohjeita tai eivät anna tehdä tietoturvatarkastuksia. (7, s. 6.)

Tietosuoja-asetus edellyttää, että rekisterinpitäjän on tehtävä tietojenkäsittelyä koskeva sopimus henkilötietojen käsittelijän kanssa. Sopimuksessa määrätään useista henkilötietoja koskevista vaatimuksista, kuten siitä, että käsittelijän tulee toimia ainoastaan rekisterinpitäjän ohjeiden mukaisesti ja toteuttaa riittävät turvatoimet, jotta pystytään estämään henkilötiedot häviämiseltä, luvattomalta kä-

sittelyltä sekä muuttumiselta. Usein on kuitenkin niin, että pilvipalveluiden tarjoajat tarjoavat palveluitaan sellaisin käyttöehdoin, että ne eivät täytä näitä vaatimuksia. (7, s. 7.)

Henkilötietoja on kerättävä niin vähän kuin tarkoituksen kannalta on tarpeen. On myös rajoitettava erityisten tietoryhmien käsittelyä. Esimerkiksi sellaisia ovat tiedot, joista käy ilmi rotu, biometrisiä ominaisuuksia, poliittisia mielipiteitä tai terveydentilaa koskevia tietoja. Samoin arkaluonteisten tietojen käsittelyä on rajoitettava, kuten verotunnistetietoja ja lapsia koskevia tietoja. Nämä edellyttävät sovellusten toimivuuden ja dataelementtien tarkkaa mietintää ennen niiden käyttöönottoa. Useat pilvipalvelujen tarjoajat ilmoittavat tietoja ja toimivuutta koskevista vaatimuksista vasta sen jälkeen, kun organisaatiot ovat alkaneet jo käyttää niitä. (7, s. 7.)

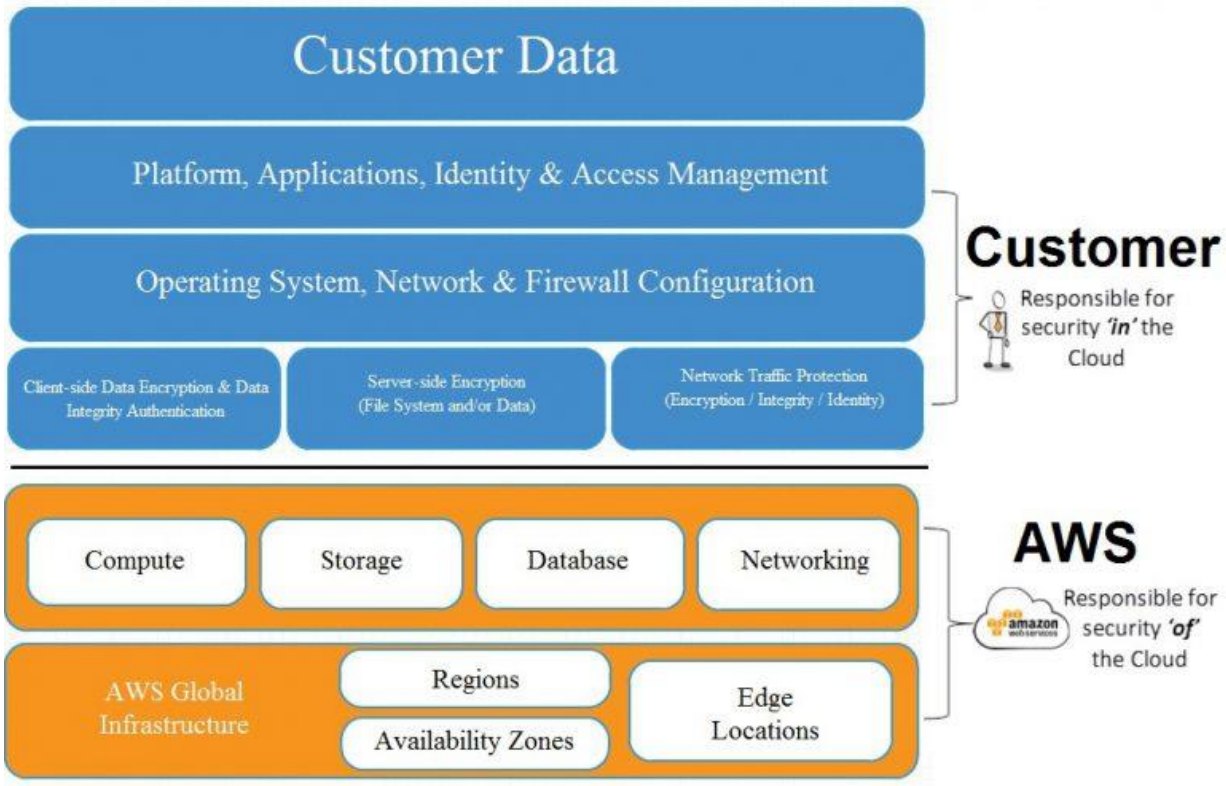
Uuden tietosuoja-asetuksen mukaan henkilötietoja ei saa käyttää muuhun kuin palveluiden tarjoamiseen asiakkaille. Monet palvelujen tarjoajat kuitenkin varaavat oikeuden käyttää tietoja toissijaisiin tarkoituksiin, kuten markkinointiin. Tämä on yleistä erityisesti silloin, kun palvelu on ilmainen. Palveluntarjoajat käyttävät tällöin tietoja saadakseen tuloja. Jotkut pilvipalveluiden tarjoajat vaativat jopa täyden omistusoikeuden niiden ympäristöönsä tallennettuihin tietoihin myydäkseen niitä eteenpäin kolmansille osapuolille. Vaikka monet näitä asioita tekevätkin, se ei ole silti luvallista. (7, s. 7.)

EU:n uusi tietosuoja-asetus edellyttää, että henkilötiedot on poistettava, kun niiden käyttötarkoitus on lakannut. Käytännössä tämä tarkoittaa sitä, että organisaatioiden on määritettävä etukäteen määräaika tietojen säilyttämiselle ja poistettava tiedot järjestelmistään automaattisesti. Voi myös toimia niin, että tietojen käyttäjä voi tehdä perustellun päätöksen jatkaa tietojen säilyttämistä. Organisaation on myös tehtävä tarkastuksia varmistaakseen, että tiedot on oikeasti poistettu. Jotkut pilvipalveluiden tarjoajista eivät kerro selkeästi tietojen poistamismenettelyistään tai kehottavat käyttäjiä itse poistamaan tiedot. Tällöin organisaatio todennäköisesti rikkoo asetusta, jos tietoja ei poisteta pilvipalveluista asianmukaisesti. (7, s. 7.)

4.1 Vastuu pilvipalvelujen tarjoajan ja asiakkaan välillä

Julkisen pilven tietoturvan vastuu on jaettu pilvipalvelun tarjoajan ja asiakkaan välillä. Julkinen pilvi (public cloud) tarkoittaa jonkun palveluntarjoajan ylläpitämää ja useiden käyttäjien jakamaa ympäristöä, jonka voi hankkia verkosta käyttöönsä kuka tahansa. Pilvipalveluiden tarjoajia ovat mm. Amazon Web Services (AWS), Microsoft Azure, IBM ja VMware. (12.)

Palveluntarjoaja vastaa vain tiettyyn pisteeseen asti tietoturvasta. Palveluntarjoaja vastaa esimerkiksi konesalin fyysisestä tietoturvasta, verkon palomuurin konfiguroinnista ja virtualisointitason tietoturvasta. Asiakas vastaa sitten kaikesta tämän virtualisointikerroksen yläpuolella olevasta eli käyttöjärjestelmistä, sovelluksista ja datasta (kuva 5). (12.)



KUVA 5. Pilven tietoturvan jaettu vastuu. (13)

Kun tapahtuu tietomurto, jossa asiakkaan pilvessä oleva data joutuu murron kohteeksi, vastuu on asiakkaan, ei palveluntarjoajan. Ei ole merkitystä, missä tai kenellä palveluntarjoajalla data oli, vaan vastuu on asiakasyrityksellä. Tämä kannattaa ottaa huomioon mietittäessä tietoturvaratkaisuja. (12.)

5 OHJEITA MEDIRACERILLE

Mediracer Oy on terveysteknologia-alan yritys, joka perustettiin vuonna 2002. Yritys on kehittänyt perusterveydenhuollon käyttöön suunnatun Point of Care (PoC) -hermoratatutkimuslaitteen. Point of Care -laitteella tarkoitetaan sellaista laitetta, jolla sairaanhoitaja tai lähihoitaja voi mitata potilasta omassa hoitohuoneessaan. Laitteella mitataan hermopinteitä sähköstimulaation avulla. Yritykselläoli tarve perehtyä EU:n uuteen tietosuoja-asetukseen. Asia nousi esille ohjelmistokehitysprojektin myötä. Jo projektin aikana arkkitehtuuria mietittäessä on hyvä ottaa tietosuoja-asiat huomioon. Järjestelmään kuuluu lausuntopalvelu, jossa säilytetään potilastietoja, ja tältä osin Mediracer luetaan valmistajana rekisterinpitäjäksi.

Ohjeistuksen puuttuessa Mediracer ei ole voinut tehdä suunnitelmaa tietosuojan osalta. Aluksi suositellaan tehtäväksi DPIA (Data Protection Impact Assessment) eli henkilötietoja koskevien tietojen vaikutusarviointi. Se ei ole yrityksille pakollinen, mutta se on suositeltavaa tehdä. Alussa kannattaisi selvittää ainakin,

1. mikä tieto on henkilötietoa
2. mitä henkilötietoja kerätään ja käsitellään
3. onko käsittely nykyisen henkilötietolain mukaista
4. ovatko henkilötiedot tarpeellisia määriteltyyn tarkoitukseen
5. miten tiedottaa rekisteröidyille heidän tietojensa käsittelystä
6. mikä on suunniteltu tietojen säilytysaika
7. mitä toimintatapoja, prosesseja ja dokumentteja tulisi asetuksen myötä muuttaa tai luoda
8. missä organisaation palvelimet ja data sijaitsevat. (10.)

Tämän jälkeen olisi hyvä tietenkin tehdä kokonainen kaiken kattava tietosuojaohjelma. Kuvassa 6 on hyvin tiivistetty erilaisia kysymyksiä, jotka organisaation johdon olisi hyvä käydä läpi, ennen kuin uusi tietosuoja-asetus tulee voimaan.

KUVA 6. Konkreettisia valmistautumiskysymyksiä yritysjohdolle (14)

5.1 Varautuminen tietomurtoon

Nykypäivänä yrityksen on pakko varautua tietomurtoon, sillä se tulee tapahtumaan ennemmin tai myöhemmin. Tänä päivänä ei voida enää ajatella, että estetään hyökkäys, vaan pitää ajatella ennemminkin, että joku on jo sisällä. Aiemmin ajateltiin puolustusta linnojen rakentamisena, kun taas kehittyneempi ajatus siitä on yrittää puolustautua kerroksittain, muistuttaen sipulin rakennetta. Syynä tähän on nykyjärjestelmien monimutkaisuus sekä entistä ammattimaisemmat hyökkääjät. (15.)

Hyökkääjät yrittävät murtautua taukoamatta. Heidän tarvitsee päästä vain kerran läpi, kun taas puolustajana pitää onnistua estämään kaikki hyökkäykset. Siihen voi riittää yksi saastunut linkki tai liite. Koulutuksista ja oppaista huolimatta

ihmiset tulevat aina avaamaan haitallisia linkkejä ja sivustoja. Ihminen on aina tietojärjestelmän heikoin lenkki. (16.)

Tietomurtoon varautumiseen on kaksi tärkeää menetelmää. Ei voida luottaa ainoastaan virustorjuntaohjelmiin ja tietoturvapäivityksiin, vaan pitää rakentaa monta tietoturvan eri kerrosta. Tämän lisäksi tilannetta pitää tarkkailla ja valvoa jatkuvasti, jotta murrot huomataan. Useamman kerroksen hyöty on siinä, että sillä voidaan estää iso osa murroista sekä lisääntyneen aktiivisuuden takia murto havaitaan ajoissa, ennen kuin koko verkko murretaan ja yrityksen tiedot kopioidaan. Tärkeää on myös selvittää, kuka hyökkää, mitä kautta ja kuinka pitkälle se on edennyt. Jos hyökkääjää ei saada selville, hyökkäys tulee todennäköisesti tapahtumaan uudelleen. Niin suojattua järjestelmää ei ole olemassakaan, johon ei voitaisi murtautua, jos hyökkääjällä on tarpeeksi resursseja ja motivaatiota. (16.)

Hyvä keino selvittää oman organisaation tietojärjestelmien tietoturvataso on testata se tunkeutumalla omiin järjestelmiin. Sen voi myös antaa ulkopuoliselle tehtäväksi, mutta silloin on tärkeää laatia turvallisuussopimus yrityksen kanssa. Laissa sanotaan, että kun testeihin on omistajan lupa, se voidaan teettä myös ulkopuolisella palveluntarjoajalla. (17.)

5.2 Toimiminen tietomurron sattuessa

Kaikesta varautumisesta huolimatta järjestelmät voivat joutua tietomurron kohteeksi. Organisaation olisi hyvä käydä läpi, miten murto oli mahdollinen ja miten tietoturvakontrolleja voitaisiin kehittää. Palautekeskustelujen olisi hyvä olla kirjattuna prosessiohjeisiin. Harva organisaatio haluaa tuoda esiin tietomurron kohteeksi joutumistaan, mutta toimintatapojen parantamisen kannalta se olisi erittäin suotavaa. Näin voitaisiin ehkäistä samalla menetelmällä tunkeutuminen toisten organisaatioiden tietoihin. (17.)

Tietoturvaloukkauksen havainnon jälkeen on tärkeää toimia harkiten ja johdonmukaisesti, jotta se onnistutaan selvittämään. Ensimmäinen ja hyvin oleellinen asia on, että ei saa hätääntyä. Olisi hyvä pitää kirjaa tehdyistä toimista, jotta

myöhemmin hyökkääjien toimet voidaan erottaa ylläpitäjien tekemistä toimista. Myös taustatietojen kerääminen tapahtumasta ja laitteista olisi hyvä kirjata ylös. Liitteessä 1 on esimerkki tapahtumapäiväkirjasta, jota Mediracer voi hyödyntää tietojen kirjaamisessa. (18.)

5.3 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Henkilötietojen tietoturvaloukkauksen sattuessa rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava perusteltu selvitys valvontaviranomaiselle. (11, s. 52.)

Henkilötietojen käsittelijää artikla 33 koskee siten, että sen on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa. Näin ollen rekisterinpitäjän vastuu on selvästi tarkemmin määritelty kuin henkilötietojen käsittelijän vastuu. (11, s. 52.)

Tietosuoja-asetuksen 33 artiklan kohdassa 3 on määritelty, mitä tietoja rekisterinpitäjän on ilmoituksessa vähintään kuvattava. Ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkaus eli eriteltävä, mitä rekisteröityjä, rekisteröityjä ryhmiä, käyttäjämääriä, henkilötietotyyppejä ja lukumääriä tietoturvaloukkaus koskee. On myös ilmoitettava tietosuojavastaavan nimi ja yhteystiedot lisätietojen saamista varten. On kuvattava todennäköiset seuraukset tietoturvaloukkauksesta sekä kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai toteuttanut tietoturvaloukkausten johdosta. Liitteessä 2 on esimerkki valvontaviranomaisille suunnatusta tietoturvaloukkauksen ilmoituslomakkeesta. (11, s. 52.)

33 artiklan 5 kohdassa vielä sanotaan, että rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset. Tämä kohta asettaa tiettyjä velvoitteita niihin tietoteknisiin ratkaisuihin, joilla henkilötietojen tietoturvaloukkauksia

pystytään seuraamaan ja dokumentoimaan ja dataa hyödyntämään ilmoitusvelvollisuuden tullessa voimaan. (11, s. 52.)

5.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidyille

Uutena velvollisuutena rekisterinpitäjille tulee velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista henkilökohtaisesti niille rekisteröidyille, joita loukkaus koskettaa. Ilmoitus on tehtävä, jos loukkaus aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille. Esimerkkejä tällaisista voisivat olla maksuvälinepetokset ja identiteettivarkaudet. Ilmoitusta ei tarvitse lähettää, jos vuotaneet henkilötiedot on salattu ja salausavaimet eivät ole vaarantuneet. Jos henkilökohtaisten ilmoitusten lähettäminen vaatii kohtuutonta vaivaa, voi rekisterinpitäjä ilmoittaa vuodosta myös median välityksellä. Tällainen tilanne voisi olla suuren kokoluokan tietovuoto, johon kuuluu lukemattomia rekisteröityjä. (4, s. 17.)

Ilmoitus tulee lähettää rekisteröidyille ilman aiheetonta viivytystä. On suositeltavaa tehdä ilmoituspohja osaksi rekisterinpitäjän kriisiviestintää. Ilmoituksessa tulisi kertoa vähintään alla luetellut kohdat. Liitteestä 3 löytyy esimerkki rekisteröidyille suunnatusta tietoturvaloukkauksen ilmoituspohjasta, jota Mediracer voi käyttää omassa toiminnassaan. (4, s. 17.)

- Selkeä ja yksinkertainen kuvaus tapahtuneesta.
- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta rekisteröidyt voivat halutessaan kysyä lisätietoja.
- Tiedot siitä, millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille.
- Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla. (4, s. 17.)

6 KEHITTÄMINEN

Koko tietosuojaprosessi vaatii jatkuvaa kehitystä. Ei riitä, että panostetaan vain muutoksen ja valmistautumisen ajan, vaan työ jatkuu myös sen jälkeen. Hyvä lähestymistapa tähän on PDCA-sykli eli jatkuvan kehittämisen kehä (kuva 7). PDCA tulee englannin kielen sanoista Plan, Do, Check ja Act. Tätä kutsutaan myös Demingin tai Shewhartin kehittymiskehäksi tai -ympyräksi. PDCA-kehä voidaan ajatella myös spiraalina, jossa kehitys nähdään päätymättömänä prosessina. Siinä toisiinsa kytkeytyneet vaiheet seuraavat toisiaan nousten yhä korkeammalle kehityksen tasolle. (19.)

KUVA 7. PDCA-sykli eli jatkuva prosessi (19)

Tässäkin asiassa, kuten monessa muussakin organisaation toiminnassa, kannattaa pyrkiä prosessimuotoiseen toimintaan. Mitä enemmän tietoturva ja tietosuoja-asiat tapahtuvat prosessimaisesti tai osana muita prosesseja, sitä helpompaa ne ovat saada osaksi yritystä. On mahdollista saada myös kustannus-

säästöjä, kun tämän hetken ohjelmisto- ja järjestelmäprojekteissa tehdään tietosuoja- ja tietoturva-asiat uuden asetuksen mukaisesti. Tällöin vältytään siltä, että keväällä 2018 huomataan puutteita ja niihin pitäisi tehdä muutoksia. Muutostyöt kun tulevat huomattavasti kalliimmaksi. (20.)

Organisaation johdon osallistuminen tietosuoja-asioihin on erittäin tärkeää. On väärin sysätä tietosuoja- ja tietoturva-asioita täysin esimerkiksi IT-osaston vastuulle, vaikka nykypäivänä se onkin aika tavallista. Olennaisena osana koko systeemin toimivuutta tähän kuuluu henkilöstön kouluttaminen ja viestintä. Koko organisaation pitää olla tietoisia tietosuoja-asetuksesta ja edes jollain tasolla ymmärtää sitä. Median paine voi olla valtava keväällä 2018, kun henkilötietosuoja-asioiden pitäisi olla yrityksillä kunnossa. Jos yritys on nukahtanut tai unohtanut koko asian, on todennäköistä, että sitä riepotellaan julkisuudessa. Tämä on hyvä muistaa ja pitää mielessä. (20.)

Yrityksen on huomioitava valmistautuessaan muutokseen riittävä resursointi niin henkilöstön panostusta kuin talouttakin ajatellen. Mahdollisuus on myös käyttää ulkopuolisia asiaan perehtyneitä lakitoimistoja, jolloin asia tulee varmasti hoidettua ja oman henkilöstön aika jää muuhun käyttöön. (20.)

Osana tietosuojaan liittyvää työtä on myös dokumenttien päivitys ja raportointi. Rekisteriselosteet ja sopimukset tulee käydä läpi ja päivittää ajan tasalle. Ajan hallinnan kannalta kannattaa aloittaa laskemalla eri sopimusten määrä, niin on helpompi arvioida, kuinka paljon siihen kuluu aikaa. Tietosuoja-asetukseen liittyviä ohjeistuksia, konkreettisia esimerkkejä ja ennakkotapauksia tullaan tulevaisuudessa kertomaan lisää, joten aktiivinen ohjeiden seuranta ja alan artikkeleiden sekä uutisten lukeminen on tärkeää. (20.)

Hyvä lähtökohta valmistautuessa uuteen tietosuoja-asetukseen on tunnistaa nykytilanne ja suhteuttaa muutos siihen. On hyvä tehdä nykytilanneselvitys, josta nähdään, kuinka iso prosessi muutos tulee olemaan. Näin osataan suunnitella ja varautua paremmin tulevaisuuteen. Organisaation kannattaa aloittaa uuden tietosuoja-asetuksen muutoksiin liittyvä projekti. Projektilla on olemassa jo selvä

päämäärä ja tavoite eli keväällä 2018 saavuttaa EU:n uuden tietosuoja-asetuksen mukaiset vaatimukset. Projektin päätyttyä jatketaan PDCA-syklin mukaisesti toimintaa eli suunnitellaan, toteutetaan, arvioidaan ja toimitaan. (20.)

7 POHDINTA

Opinnäytetyön toisen osan tarkoituksena oli tutkia, miten Mediracerin tulisi valmistautua uuteen EU:n tietosuoja-asetukseen. Työssä pohdittiin valmistautumista prosessien kannalta ja erityisesti tietomurron näkökulmasta. Pilvipalveluiden tietosuoja-asiat koettiin myös tärkeäksi ja ne otettiin työhön mukaan.

Työ eteni hyvin ja aikataulussa. Tuleva ulkomaanmatka antoi mukavasti motivaatiota työn etenemiselle. Ohjaajiltani sain hyvin apua ja vinkkejä työhöni niin kirjoittamisessa kuin tietosuoja-asioissakin.

Aiempi kokemus itselläni tietosuoja-asioista oli hyvin vähäinen. Opinnäytetyön kautta pääsin tutustumaan aiheeseen tarkemmin ja uskon hyötyväni näistä tiedoista ja taidoista myös tulevaisuudessa. Osaan ottaa tietosuoja- ja tietoturva-asiat paremmin huomioon niin arjessa kuin työelämässäkin.

Haasteita opinnäytetyössä oli lakiteksti ja sen ymmärtäminen sekä referointi työhön. Onneksi lähdemateriaaleja löytyi hyvin, vaikka asetuksen asettamisesta on melko vähän aikaa. Haasteita oli myös tekstin rakenteen ja jäsentelyn miettimisessä.

Mielestäni tavoitteisiin päästiin ja olen tyytyväinen työni tuloksiin. Opin paljon yleisesti tietosuojasta ja uutta asiaa tuli myös tietoturvan osalta. Toivon, että Mediracerkin hyötyisi tästä selvityksestä ja he saisivat vinkkejä, miten lähteä kehittämään tietosuoja-asioita omassa organisaatiossaan.

LÄHTEET

1. Salminen, Markus 2009. Tietosuoja sähköisessä liiketoiminnassa. Helsinki: Talentum.

2. Ylipartanen, Arto 2016. EU:n tietosuoja-asetuksen voimaantulo ja vaikutukset. PowerPoint-diasarja. Tietosuojavaltuutetun toimisto. Saatavissa: https://koulutus.fcg.fi/Portals/2/S03-Ylipartanen.pdf. Hakupäivä 7.3.2017.

3. Yleistä tietosuojasta. 2016. OpiTietosuojaa.fi. Saatavilla: https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja. Hakupäivä 1.3.2017.

4. EU-tietosuojan kokonaisuudistus – VAHTI-raportti. 2016. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229. Hakupäivä 9.3.2017.

5. Tiivis tietoturvasanasto. 2004. Sanastokeskus TSK ry. Saatavissa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf. Hakupäivä 27.3.2017.

6. L 19.12.1889/39. Rikoslaki. 38 luku (21.4.1995/578) Tieto- ja viestintärikoksista. 8 § (10.4.2015/368) Tietomurto. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38. Hakupäivä 21.3.2017.

7. EU:n uusi yleinen tietosuoja-asetus ja pilvipalveluihin liittyvien haasteiden hallinta. 2016. Netskope. Saatavilla: http://ymon.fi/materiaalit/pdf/EU%20GDPR%20Finnish.pdf. Hakupäivä 8.3.2017.

8. Eronen, Heidi 2016. 7 tapaa, miten EU:n tietosuoja-asetus vaikuttaa ohjelmistoyrityksiin. Planeetta Internet -blogi. Saatavilla: http://blog.planeetta.net/7-tapaa-miten-eun-tietosuoja-asetus-vaikuttaa-ohjelmistoyrityksiin. Hakupäivä 13.3.2017.

9. Pietikäinen, Suvi 2016. Rekisteröidyn oikeudet. VAHTI-raportti 1/2016. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/web/guest/rekisteroidyn-oikeudet. Hakupäivä 28.3.2017.

10. Luomala, Anette – Warma, Eija 2016. Miten valmistautua EU:n uuden tietosuoja-asetuksen vaatimuksiin? Asianajotoimisto Castrén & Snellman. Saatavissa: http://www.castren.fi/fi/blogijauutiset/blogi-2016/miten-valmistautua-eun-uuden-tietosuoja-asetuksen-vaatimuksiin/. Hakupäivä 14.3.2017.

11. (EU) 2016/679. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti). Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI. Hakupäivä 14.3.2017.

12. EU:n uuden tietosuoja-asetuksen vaikutukset yrityksiin -webinaarin linkit sekä Q&A. 2016. Centero. Saatavissa: http://www.centero.fi/blogi/3142/. Hakupäivä 16.3.2017.

13. The ABC's of the Shared Responsibility Model. 2016. Trend Micro. Saatavissa: https://www.trendmicro.com/aws/aws-shared-security-model/. Hakupäivä 20.3.2017.

14. Von Bonin, Aino 2016. Tietosuoja-asetuksen uudistus puhuttaa ja pelottaa – mistä lääkkeet tulevaan? Datacenter. Saatavilla: http://blogi.datacenter.fi/tietosuoja-asetuksen-uudistus-puhuttaa-ja-pelottaa-mist%C3%A4-l%C3%A4%C3%A4kkeet-tulevaan. Hakupäivä 17.3.2017.

15. Saarelainen, Ari 2016. Harvinaisen hyvä merkki: ”Hups, olemme tietomurron kohteena!”. Tivi. Saatavissa: http://www.tivi.fi/Kaikki_uutiset/harvinaisen-hyva-merkki-hups-olemme-tietomurron-kohteena-6536241. Hakupäivä 22.3.2017.

16. Hämäläinen, Jouni 2016. Tietomurto tapahtuu – varaudu siihen. Combitech Oy. Saatavissa: https://medium.com/@combitech/tietomurto-tapahtuu-varaudu-siihen-d5cf7800bfdb#.w2oyzwqjl. Hakupäivä 22.3.2017.

17. Lagus, Antti J. 2013. Tietomurrot: Entä jos meille murtaudutaan? Tietosuoja – Tietoturvan ja tietosuojan erikoislehti. Saatavissa: https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3230. Hakupäivä 22.3.2017.

18. Nuopponen, Antti 2013. Mitä tehdä jos epäilet joutuneesi tietomurron kohteeksi? Nixu OyJ:n TigerTeam kyberturvablogi. Saatavissa: https://www.nixu.com/fi/blogi/2013-02/mit%C3%A4-tehd%C3%A4-jos-ep%C3%A4ilet-joutuneesi-tietomurron-kohteeksi. Hakupäivä 22.3.2017.

19. Laatutyökaluja. 2010. Laatuakatemia. Saatavissa: http://www.koti-posti.net/tuurala/PDCA.htm. Hakupäivä 23.3.2017.

20. Rousku, Kimmo 2016. Mitkä ovat raportin suositukset, miten tästä eteenpäin? Livestream. Valtionvarainministeriö. Saatavissa: https://livestream.com/ITstriimIT/VAHTI-tietosuoja/videos/124882393. Hakupäivä 23.3.2017.

TAPAHTUMAPÄIVÄKIRJAN MALLI

Tähän päiväkirjaan voidaan kirjata tietoturvaloukkauksiin liittyvät toimenpiteet ja tapahtumat.

Tietoturvaloukkauksen kohde_____

Selvitysryhmän jäsenet ja yhteystiedot_____

_____

Aika	Havainto/ Tapahtumakuvaus	Vastuuhen-kilö	Tehdyt toimenpiteet	Kommentit

VALVONTAVIRANOMAISELLE SUUNNATTU TIETOTURVA-LOUKKAUKSEN ILMOITUSLOMAKKEEN MALLI

Tällä lomakkeella voidaan ilmoittaa organisaatiossa tapahtuneesta tietoturva-loukkauksesta valvontaviranomaiselle.

Ilmoittaja_____

Yritys_____

Tietoturvaloukkauksen kuvaus

Tapahtuma-ajankohta
Tapahtumapaikka/ -kohde
Loukkauksen tyyppi (tietomurto, tietovuoto, tietojen kalastelu jne.)
Tapahtumakuvaus (havainnot, ketä koskee yms.)
Aiheutuneet vahingot ja mahdolliset seuraavat vahingot
Toteutetut toimenpiteet ja jatkotoimenpiteet
Tietosuojavastaavan yhteystiedot

REKISTERÖIDYILLE SUUNNATTU TIETOTURVALOUKKAUKSEN ILMOITUSLOMAKKEEN MALLI

Tällä lomakkeella voidaan ilmoittaa organisaatiossa tapahtuneesta tietoturvaloukkauksesta rekisteröidyille.

Ilmoittaja_____

Yritys_____

Tietoturvaloukkauksen kuvaus

Tapahtuman kuvaus
Mahdolliset vaikutukset rekisteröidyille
Toteutetut toimenpiteet ja jatkotoimenpiteet
Tietosuojavastaavan yhteystiedot